Construction of Hurwitz Spaces and Applications to the Regular Inverse Galois Problem

Kenji Sakugawa

January 11, 2012

1 Introduction

A famous open problem in Number theory called Inverse Galois Problem is as follows.

Question 1.1. (IGP) Does every finite group occurs as the Galois group of a finite Galois extension over $\mathbb{Q}$?

The same statement as IGP is always expected to be true when we replace $\mathbb{Q}$ by any algebraic number field which is a Hilbertian field(see [Se, Def. 3.1.3.] for the definition Hilbertian fields).

We do not recall the definition of Hilbertian fields, but we recall that any finite number field F is Hilbertian. There are some algebraic number fields F of infinite degree over $\mathbb{Q}$ which are Hilbertian (e.g. the maximal abelian extension $\mathbb{Q}^{\mathrm{ab}}$ of $\mathbb{Q}$ is a Hilbertian fields. We will denote by IGP_F the analogue of the inverse Galois problem for a Hilbertian field F.

We consider the following variant of the problem IGP.

Question 1.2. (RIGP_F) Let F be any field. Does every finite group G occur as geometrically connected G-covering of $\mathbb{P}^1_F$?

For a finite group G, we call a finite flat morphism of schemes $f : X \to W$ the G-covering if G acts X over W and if f induces the isomorphism $X/G \xrightarrow{\sim} W$. We say that G is regular over F if there exists a geometrically connected G-covering over $\mathbb{P}^1_F$. The above question is called the regular inverse Galois problem over F (RIGP_F).

The following proposition is an immediate consequence of Hilbert's irreducibility theorem.

Proposition 1.3. *Let F be a Hilbertian field. Then, IGP holds for F if RIGP holds for F.*

The advantage of considering RIGP instead of IGP is that RIGP admits a purely group theoretic approach. In other words, we get a purely group theoretic

sufficient condition of regularity of G. In [Th], Thompson proved the following theorem.

Let $\mathcal{C} = (C_1, \dots, C_r)$ be an r-tuple of conjugacy classes of G. Put

$$\mathcal{E}^{\mathrm{in}}(\mathcal{C}) := \{(g_1, \dots, g_r) \in G^r \mid g_i \in C_i,\ g_1 \dots g_r = 1,\ \langle g_1, \dots, g_r\rangle = G\}/\mathrm{Inn}(G)$$

and define an abelian extension $\mathbb{Q}_{\mathcal{C}}$ of $\mathbb{Q}$ by

$$\mathrm{Gal}(\overline{\mathbb{Q}}/\,\mathbb{Q}_{\mathcal{C}}) := \mathrm{Stab}_{G_{\mathbb{Q}}}(\{\mathcal{C}_1, \dots, \mathcal{C}_r\})$$

(see Definition 2.9 for the action of $G_{\mathbb{Q}}$ on $\{\{\mathcal{C}_1^n, \dots, \mathcal{C}_r^n \mid n \in \mathbb{Z}_{>0}\ ,\ (n, |G|) = 1\})$.

Proposition 1.4. *[Th]*(Rigidity method.) If there exists a natural number r and an r-tuple of conjugacy class $\mathcal{C}$ of G such that $|\,\mathcal{E}^{\mathrm{in}}(\mathcal{C})| = 1$, then G is regular over $\mathbb{Q}^{\mathrm{ab}}$. Moreover $G/Z(G)$ is regular over $\mathbb{Q}_{\mathcal{C}}$.

We will give the proof of the above proposition in 2.1 in a slightly different way from that of [Th]. The proof of this proposition will be related to an essential step of the proof of our main results explained below.

In the paper [Fr-Vö], Fried and Völklein considered the set of equivalence classes

$$\mathcal{H}_r^{\mathrm{in}}(G)(\mathbb{C}) := \{\text{G-coverings over } \mathbb{P}^1_{\mathbb{C}} \text{ ramified at exactly } r\text{-points on } \mathbb{P}^1_{\mathbb{C}}\}/\sim .$$

Here, we call coverings $f : X \to \mathbb{P}^1_{\mathbb{C}}$ and $g : Y \to \mathbb{P}^1_{\mathbb{C}}$ are equivalent if there exists an isomorphism for X to Y over $\mathbb{P}^1_{\mathbb{C}}$.

Fried and Völklein obtain the following theorem.

Proposition 1.5. *[Fr-Vö]Let G, r be as above .*
(1) There exists an algebraic variety $\mathcal{H}_r^{\mathrm{in}}(G)$ over $\mathbb{Q}$whose $\mathbb{C}$-valued points are canonically identified with $\mathcal{H}_r^{\mathrm{in}}(G)(\mathbb{C})$.
(2) Let L be an extension of $\mathbb{Q}$. Suppose that the center of G is trivial. Then, there exists a geometrically connected G covering over $\mathbb{P}^1_L$ if and only if $\mathcal{H}_r^{\mathrm{in}}(G)(L)$ is not empty.
(3) Let L be an extension of $\mathbb{Q}$ whose absolute Galois group G_L has cohomlogical dimension≤ 1. Then, the same equivalence as that of (2) holds without any assumption of G.

We call $\mathcal{H}_r^{\mathrm{in}}(G)$ the Hurwitz space.

It is not difficult to see that there exists an algebraic variety $\mathcal{H}_r^{\mathrm{in}}(G)_{\mathbb{C}}$ whose $\mathbb{C}$-valued points are identified with $\mathcal{H}_r^{\mathrm{in}}(G)(\mathbb{C})$.
Fried and Völklein tried to prove that $\mathcal{H}_r^{\mathrm{in}}(G)_{\mathbb{C}}$ is the moduli space of G coverings over a projective line ramifying at exactly r-points. This implies that the field of definition of $\mathcal{H}_r^{\mathrm{in}}(G)_{\mathbb{C}}$ is equal to $\mathbb{Q}$. Actually, they proved the representability of a certain auxiliary moduli problem $\mathcal{H}^{\mathrm{ab}}(G, U)$ in the special case (see [Fr-Vö, Section 1.2.]), but to solve RIGP for G, it is enough to prove that $\mathcal{H}_r^{\mathrm{in}}(G)_{\mathbb{C}}$ is defined over $\mathbb{Q}$.

In this paper, we give a simpler construction of the Hurwitz spaces. Thanks to our new construction, we generalize Thompson's rigidity method as follows:

Main Theorem A . *(Theorem 3.2, Theorem 3.3, Theorem 3.4.)Let G be a finite group and r be a positive integer.*
(1) Assume that there exists an r-tuple of conjugacy classes $\mathcal{C}$ of G and a subgroup $H \subset \mathrm{Aut}_{\mathcal{C}}(G)$ which satisfy the following conditions:
(a) The subgroup $H \subset \mathrm{Aut}_{\mathcal{C}}(G)$ acts on $\mathcal{E}^{\mathrm{in}}(\mathcal{C})$ transitively .
(b) The subgroup H is an abelian group or a dihedral group D_n.
Then, G is regular over $\mathbb{Q}^{\mathrm{ab}}$.
(2) Assume the conditions (a) and (b). Let m be the number defined by

$$m := \begin{cases} \text{the exponent of } H & \text{if } H \text{ is abelian.} \\ n & \text{if } H = D_n. \end{cases}$$

Then $G/Z(G)$ is regular over $\mathbb{Q}_{\mathcal{C}}(\mu_m)$.
(3) Assume the conditions (a) and (b). If the inclusion from H to $\mathrm{Aut}_{\mathcal{C}}(G)$ can be extended to a group homomorphism from $(\mathbb{Z}/m\mathbb{Z})^\times \ltimes H$ into $\mathrm{Aut}_{\mathcal{C}}(G)$ and if the action of $(\mathbb{Z}/m\mathbb{Z})^\times$ on $\mathcal{E}^{\mathrm{in}}(\mathcal{C})$ is trivial, then $G/Z(G)$ is regular over $\mathbb{Q}_{\mathcal{C}}$.
(4) Assume the conditions (a) and (b). If $H \subset D_4$ and the action of H on $\mathcal{E}^{\mathrm{in}}(\mathcal{C})$ factors through $H \subset D_4 \twoheadrightarrow (\mathbb{Z}/2\mathbb{Z})^2$ and the action of H can be extended to an action of D_4, then $G/Z(G)$ is regular over $\mathbb{Q}_{\mathcal{C}}$.

Next, we obtain an application of our first main theorem as follows.

Corolally A . *(Proposition 3.35.)Let p be an odd prime and n be an even natural number. If $p \equiv 7(\mod 12), 4|n$ and $n \geq 12$, then $PSO_n^+(\mathbb{F}_p)$ is regular over $\mathbb{Q}$.*

To prove Corollary A, we use middle convolution functors and scalar multiplications which are defined in the paper [D-R, Section 3.2]. Let r be a positive integer and K be a field. Let $\mathcal{F}_r$ be a free group of rank r and $\mathrm{Rep}_K(\mathcal{F}_r)$ be the category of finite dimensional linear representations of $\mathcal{F}_r$ over K. We use middle convolution functors $\mathrm{MC}_\lambda^{(r)}$ for $\lambda \in K^\times$ and scalar multiplication functors $\mathrm{M}_\Lambda^{(r)}$ for $\Lambda \in (K^\times)^r$ which are defined in the paper [D-R]:

$$\mathrm{MC}_\lambda^{(r)}, \mathrm{M}_\Lambda^{(r)} : \mathrm{Rep}_K(\mathcal{F}_r) \to \mathrm{Rep}_K(\mathcal{F}_r).$$

The functors $\mathrm{MC}_\lambda^{(r)}, \mathrm{M}_\Lambda^{(r)}$ satisfy the following conditions:
(*) Let $\mathcal{R}$ be a full subcategory of $\mathrm{Rep}_K(\mathcal{F}_r)$ which is defined in Lemma 3.23. Then $\mathrm{MC}_\lambda^{(r)}$ and $\mathrm{M}_\Lambda^{(r)}$ induce category equivalences $\mathcal{R} \cong \mathcal{R}$ and quasi -inverses are $\mathrm{MC}_{\lambda^{-1}}^{(r)}$ and $\mathrm{M}_{\Lambda^{-1}}^{(r)}$

We prove also the regularity of $PSO_n^+(\mathbb{F}_p)$ when n is even and not divided 4. However in this case, we can not apply Main Theorem A. We use the theory of the action of braid groups which are also considered in the paper [D-R, Section 4.1]. The most important property of the action of braid groups is that they commute with $\mathrm{MC}_\lambda^{(r)}$ and $\mathrm{M}_\Lambda^{(r)}$. In section 4,2, we obtain the following theorem.

Main Theorem B . *(Theorem 4.11.)Let $\mathbb{T} = (T_1, \ldots, T_r)$ be an r-tuple of elements of $GL_n(\mathbb{F}_q)$ as Lemma 4.5. Let $\tilde{\mathbb{T}}$ be an r-tuple which arises an iterated*

application of middle convolutions and scalar multiplications to $\mathbb{T}$*. Denote* $\tilde{\mathbb{T}}$ *by* $(\tilde{T}_1, \dots, \tilde{T}_r)$*. Assume that the* r*-tuple conjugacy classes* $(C(\tilde{T}_1), \dots, C(T_r))$ *of* $\langle\, \tilde{\mathbb{T}} \,\rangle$ *is rational. Here* $C(T_i)$ *is the conjugacy class of* $\langle\, \tilde{\mathbb{T}} \,\rangle$ *such that* $C(T_i)$ *contains* T_i*. If there exists a subgroup* $H \subset N_{GL_m(\mathbb{F}_q)}(\langle\, \tilde{\mathbb{T}} \,\rangle)$ *such that the image of* H *in* $N_{GL_m(\mathbb{F}_q)}(\langle\, \tilde{\mathbb{T}} \,\rangle)/\langle\, \tilde{\mathbb{T}} \,\rangle$ *is equal to* $N_{GL_m(\mathbb{F}_q)}(\langle\, \tilde{\mathbb{T}} \,\rangle)/\langle\, \tilde{\mathbb{T}} \,\rangle$ *and satisfies one of the following conditions:*
(a) The group H *is isomorphic to a product of several copies of* $\mathbb{Z}/2\,\mathbb{Z}$*.*
(b) The group H *is isomorphic to* $(\mathbb{Z}/2\,\mathbb{Z})^2 \rtimes S_2 = D_4$ *and the action of* H *on* $\mathcal{E}^{\mathrm{in}}(\mathcal{C})$ *factors through the canonical projection* $H \twoheadrightarrow H/\langle (1,1) \rangle \cong (\mathbb{Z}/2\,\mathbb{Z})^2$*.*
Then $\langle\, \tilde{\mathbb{T}} \,\rangle$ *is regular over* $\mathbb{Q}$*.*

We prove the following corollary in Section 4.2, as a consequence of Main Theorem B.

Corolally B . *Let* p *be an odd prime and* n *be an even natural number.*
(1) (Proposition 4.12.) If $p \equiv 7(\mod 12), 4 \nmid n$ *and* $n \geq 12$*, then* $PSO_n^+(\mathbb{F}_p)$ *is regular over* $\mathbb{Q}$*.*
(2) (Proposition 4.14.) Let q *be a power of* p *and* n *be an even natural number. If* $n > max\{\varphi(q-1), 7\}, \frac{n}{2} \equiv \frac{\varphi(q-1)}{2} + 1 \;(\mod 2)$ *and* $q \equiv 3(\mod 4)$*, then* $PSO_n^+(\mathbb{F}_q)$ *is regular over* $\mathbb{Q}$*.*

Remark 1.6. *The regularities over* $\mathbb{Q}$ *of* $PSO_n^+(\mathbb{F}_q)$ *are known if* $q = p$ *,* $n \equiv 2 \pmod 4$ *and* $p \equiv 7 \pmod{12}$ *and* $p \nmid n$ *([M-M, Theorem 10.3. (i)]) or if* $n > 2\max\{\varphi(\mathrm{q}-1), 7\}$ *and* $q \equiv 3(mod\ 4)$*([D-R, Lemma 9.5.]).*

The plan of the paper is as follows:
Plan. In Section 2, we construct $\mathcal{H}_r^{\mathrm{in}}(G)$ as an etale sheaf on the configuration space $\mathcal{U}_r$ of r-points over $\mathbb{P}^1_{\mathbb{Q}}$. We regard a finite group G as the constant sheaf on $\mathcal{U}_r$. Therefore we will generalize the Hurwitz spaces by replacing constant sheaves with locally constant sheaves. We do not need the scheme $\mathcal{H}^{\mathrm{ab}}(G, U)$ which was used in [Fr-Vö]. The key of our construction is the use of the theory of the etale fundamental group of schemes in the sense of SGA1. We construct moduli spaces of G-coverings not only over $\mathbb{P}^1_{\mathbb{Q}}$ but also over some other smooth algebraic varieties (for example, elliptic curves, see Remark 2.21). The author believes that this generalization is useful to study IGP via the analogous problem to RIGP over algebraic varieties.

In Section 3.1, we prove Main Theorem A. In Section 3.2, we prepare some group theoretic lemmas to prove Corollary A and B and define middle convolution functors and scalar multiplications in Section 3.3. Next, we recall the notion of the linearly rigidity in 3.4. Then we prove Corollary A in Section 3.5.

In Section 4, we prove Main Theorem B and Corollary B. The Main tool is the theory of the action of the braid groups. In section 4.1, we prove Theorem B (Theorem 4.11) by using some results on the action of braid groups which are proved by Dettweiler and Reiter in the paper [D-R]. We prove Corollary B in Section 4.2.

Acknowledgements The author would like to thank Professor Tadashi Ochiai for reading this paper carefully and variable discussions. Also, the author would like to Professor Tetsushi Ito for some useful suggestions.

2 Construction

In Section 2, we define Hurwitz spaces and generalize Proposition 1.5.

2.1 The fundamental groups of schemes and examples

In this section, we recall the etale fundamental group of schemes and give important examples.

Theorem-definition 2.1. *[SGA1, Exposé X] Let X be a connected locally Noetherian scheme. Then there exists the unique pro-finite group $\pi_1^{\mathrm{et}}(X, \bar{x})$ and the equivalence of categories as follows:*

$$(\textit{Finite etale coverings of } X) \xrightarrow{\sim} (\textit{Finite sets which has an action of } \pi_1^{\mathrm{et}}(X, \bar{x})).$$

$$f : W \to X \qquad \longmapsto \qquad f^{-1}(\bar{x}) \qquad .$$

Here $\bar{x}$ is a geometric point of X i.e. a morphism from a spectrum of an algebraically closed field to X. If we take another geometric point $\bar{y}$, then there exists an isomorphism $\pi_1^{\mathrm{et}}(X, \bar{x}) \cong \pi_1^{\mathrm{et}}(X, \bar{y})$. This isomorphism is unique up to inner automorphisms. We call $\pi_1^{\mathrm{et}}(X, \bar{x})$ the etale fundamental group of X.

So we always identify a finite etale covering of X with a finite set which has an action of $\pi_1^{\mathrm{et}}(X, \bar{x})$.

2.1.1 Example of punctured projective line over $\mathbb{C}$

Let r be a positive integer and $X = \mathbb{P}^1_{\mathbb{C}} \setminus \{x_1, \ldots, x_r\}$, $x_i \in \mathbb{P}^1(\mathbb{C})$. By the Riemann's existence theorem, every compact Riemann surface is identified with algebraic curves over $\mathbb{C}$. In particular, every finite topological covering of X is identified with an algebraic curve over $\mathbb{C}$. Thus $\pi_1^{\mathrm{et}}(X, x)$, $x \in X(\mathbb{C})$ is isomorphic to the pro-finite completion of the topological fundamental group $\pi_1^{\mathrm{top}}(X(\mathbb{C}), x)$ of $X(\mathbb{C})$. The group $\pi_1^{\mathrm{top}}(X(\mathbb{C}), x)$ is isomorphic to the free group of rank $r-1$. This group is generated by the homotopy classes ϵ_i of a loop around x_i for each i with the relation $\epsilon_1 \epsilon_2 \ldots \epsilon_r = 1$.
Let G be a finite group. By the definition of the etale fundamental group, we identify isomorphism classes of etale G-coverings of X with G-orbit of surjective group homomorphisms $\pi_1^{\mathrm{et}}(X, x) \to G$. This proves the following lemma.

Lemma 2.2. *Let X be $\mathbb{P}^1_{\mathbb{C}} \setminus \{x_1, \ldots, x_r\}$. For a finite group G, the following sets are identified:*
(1) G-coverings of X modulo isomorphisms.
(2) $\mathrm{Surj}(\pi_1^{\mathrm{et}}(X, x), G)/\mathrm{Inn}G$.
(3) $\mathcal{E}_r^{\mathrm{in}}(G) := \{(g_1, \ldots, g_r) \in G^r | g_1 \ldots g_r = 1, \langle g_1, \ldots, g_r \rangle = G\}/\mathrm{Inn}(G)$
where $\mathrm{Inn}(G)$ *acts on* G^{r} *diagonally.*

Remark 2.3. *In general, for any algebraic variety X over $\mathbb{C}$, $\pi_1^{\mathrm{et}}(X, x)$ is canonically isomorphic to the pro-finite completion of the $\pi_1^{\mathrm{top}}(X(\mathbb{C}), x)$ (see [SGA1, Exposé 10]).*

Remark 2.4. *If X is an algebraic variety over $\overline{\mathbb{Q}}$ and fix an embedding $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$. Then the morphism $X_{\mathbb{C}} \to X$ induces an isomorphism $\pi_1^{\mathrm{et}}(X_{\mathbb{C}}, x) \xrightarrow{\sim} \pi_1^{\mathrm{et}}(X, x)$. This is proved by the technique of specialization (see [Se, Chapter 6]).*

2.1.2 Example of punctured projective line over $\mathbb{Q}$

Next, we consider an arithmetic case. Let $X = \mathbb{P}^1_{\mathbb{Q}} \setminus \{x_1, \ldots, x_r\}$ where $x_i \in \mathbb{P}^1(\overline{\mathbb{Q}})$ and the set $\{x_i\}_i$ is $G_{\mathbb{Q}}$ stable. For a field k, we denote by G_k the absolute Galois group $\mathrm{Gal}(\overline{k}/k)$ throughout this paper.

Lemma 2.5. *([SGA1] The fundamental exact sequence.) Let X be a geometrically connected algebraic variety over $\mathbb{Q}$. Then, there exists an exact sequence:*

$$1 \to \pi_1^{\mathrm{et}}(X_{\overline{\mathbb{Q}}}, \bar{x}) \to \pi_1^{\mathrm{et}}(X, \bar{x}) \to G_{\mathbb{Q}} \to 1 \ .$$

This exact sequence induces an outer action of $G_{\mathbb{Q}}$ on $\pi_1(X_{\overline{\mathbb{Q}}}, \bar{x})$ and an action of $G_{\mathbb{Q}}$ on $\mathrm{Surj}(\pi_1^{\mathrm{et}}(X, \bar{x}), G)/\mathrm{Inn}G$ for a finite group G. This action is mysterious in general. However if X is isomorphic to $\mathbb{P}^1_{\mathbb{Q}}$ minus r-points, the action of $G_{\mathbb{Q}}$ on $\pi_1^{\mathrm{et}}(X_{\overline{\mathbb{Q}}})^{\mathrm{ab}}$ is described as follows.

Lemma 2.6. *[M-M, Chapter 1,Theorem 2.6.] Let $X = \mathbb{P}^1_{\mathbb{Q}} \setminus \{x_1, \ldots, x_r\}$ where $x_i \in \mathbb{P}^1(\overline{\mathbb{Q}})$ and the set $\{x_i\}_i$ is $G_{\mathbb{Q}}$-stable. Let $\pi : G_{\mathbb{Q}} \to S_r$ be the group homomorphism so that $\tau(x_i) = x_{\pi(\tau)(i)}$ for all $\tau \in G_{\mathbb{Q}}$. Then, $\tau(C(\epsilon_i)) = C(\epsilon_{\pi(\tau)(i)})^{\chi(\tau)}, \tau \in G_{\mathbb{Q}}$. Here $C(\epsilon_i)$ is the conjugacy class of $\epsilon_i \in \pi_1^{\mathrm{et}}(X_{\overline{\mathbb{Q}}}, \bar{x})$ and $\chi : G_{\mathbb{Q}} \to \hat{\mathbb{Z}}^{\times}$ is the cyclotomic character.*

Let G be a finite group. The outer action of $G_{\mathbb{Q}}$ on $\pi_1^{\mathrm{et}}(\mathbb{P}^1_{\overline{\mathbb{Q}}} \setminus \{x_1, \ldots, x_r\}, x)$ which is induced by the fundamental exact sequence induces the action of $G_{\mathbb{Q}}$ on $\mathcal{E}^{\mathrm{in}}(G)$ via the identification of Lemma 2.2. This $G_{\mathbb{Q}}$-action on $\mathcal{E}_r^{\mathrm{in}}(G)$ can lift to $\mathcal{E}_r(G) := \{(g_1, \ldots, g_r) \in G^r | g_1 \ldots g_r = 1, \langle g_1, \ldots, g_r \rangle = G\}$ as follows. First, we take $\mathbb{Q}$-rational point y of $\mathbb{P}^1_{\mathbb{Q}} \setminus \{x_1, \ldots, x_r\}$. Since the formalism of the fundamental group is covariant, a $\mathbb{Q}$-rational point y induces a splitting of the following exact sequence:

$$1 \to \pi_1^{\mathrm{et}}(X_{\overline{\mathbb{Q}}}, \bar{x}) \to \pi_1^{\mathrm{et}}(X, \bar{x}) \to G_{\mathbb{Q}} \to 1 \ .$$

Thus, the outer action of $G_{\mathbb{Q}}$ action on the fundamental group $\pi_1^{\mathrm{et}}(X_{\overline{\mathbb{Q}}}, \bar{x})$ lifts to the action on $\pi_1^{\mathrm{et}}(X_{\overline{\mathbb{Q}}}, \bar{x})$. This action of $G_{\mathbb{Q}}$ on $\pi_1^{\mathrm{et}}(X_{\overline{\mathbb{Q}}}, \bar{x})$ induces the action of $G_{\mathbb{Q}}$ on the set $\mathrm{Surj}((\pi_1^{\mathrm{et}}(\mathbb{P}^1_{\overline{\mathbb{Q}}} \setminus \{x_1, \ldots, x_r\}, \bar{x}), G)$, and induces the action on $\mathcal{E}_r(G)$. Note that this action is independent on a choice of a rational point up to inner automorphisms of G.
Let $f : \pi_1^{\mathrm{et}}(\mathbb{P}^1_{\overline{\mathbb{Q}}} \setminus \{x_1, \ldots, x_r\}, \bar{x}) \to G$ be a surjective group homomorphism which corresponds to $[g = (g_1, \ldots, g_r)] \in \mathcal{E}_r^{\mathrm{in}}(G)$.

If $[g]$ is fixed by G_F the absolute Galois group of a number field F, then for all $\beta \in G_F$ there exists $g_\beta \in G$ such that $\beta(g_i) = g_\beta g_i g_\beta^{-1}$ for all $1 \leq i \leq r$.

Here, we fix a lift of the action of $G_{\mathbb{Q}}$ on $\mathcal{E}_r(G)$ as above.
Put $c(\alpha,\beta) := g_\alpha g_\beta g_{\alpha\beta}^{-1}$. This is a 2-cocycle of G_F whose values are in the center of G and class of c in $H^2(G_F, Z(G))$ is independent of a choice of a lift of the action of $G_{\mathbb{Q}}$ on $\mathcal{E}_r(G)$ because this lift is unique up to inner automorphisms of G.

Lemma 2.7. *Let G be a finite group and $f \in \mathrm{Surj}((\pi_1^{\mathrm{et}}(\mathbb{P}^1_{\overline{\mathbb{Q}}} \setminus \{x_1, \dots, x_r\}, \bar{x}), G)$. Let c be the 2-cocycle associated a group homomorphism f as explained above. Then f can be extended to a group homomorphism $\pi_1^{\mathrm{et}}(X_F\ , \bar{x}) \simeq \pi_1^{\mathrm{et}}(X_{\overline{F}}\ , \bar{x}) \rtimes G_F \to G$ if and only if c is a coboundary. Here, the isomorphism $\pi_1^{\mathrm{et}}(X_F\ , \bar{x}) \simeq \pi_1^{\mathrm{et}}(X_{\overline{F}}\ , \bar{x}) \rtimes G_F$ is defined by the fixed splitting of the fundamental exact sequence.*

Proof. Assume that c is a coboundary , that is, there exists a continuous map $\xi : G_F \to Z(G)$ such that $c(\beta,\gamma) = d\xi(\beta,\gamma) = \xi(\beta)\xi(\gamma)\xi(\beta\gamma)^{-1}$. Put $\tilde{f}((\tau,\beta)) := f(\tau)g_\beta\xi(\beta)^{-1}$, then $\tilde{f}$ is a group homomorphism. In fact, for any element $\tau,\mu \in \pi_1^{\mathrm{et}}(X_{\overline{F}}\ , x)$, $\beta,\gamma \in G_F$, $\tilde{f}$ is checked to be multiplicative as follows:

$$\begin{aligned}
\tilde{f}((\tau,\beta)(\mu,\gamma)) &= \tilde{f}((\tau\mu^\beta,\beta\gamma)) = f(\tau\mu^\beta)g_{\beta\gamma}\xi(\beta\gamma)^{-1} \\
&= f(\tau)f(\mu^\beta)g_{\beta\gamma}\xi(\beta\gamma)^{-1} = f(\tau)g_\beta f(\mu)g_\beta^{-1}g_{\beta\gamma}\xi(\beta\gamma)^{-1} \\
&= f(\tau)g_\beta f(\mu)g_\gamma\xi(\beta)^{-1}\xi(\gamma)^{-1} = \tilde{f}((\tau,\beta))\tilde{f}((\mu,\gamma)).
\end{aligned}$$

Conversely, if f can be extended to a group homomorphism $\tilde{f}$, c is a coboundary because of the fact that $\tilde{f}$ is multiplicative. □

Lemma 2.8. *Notation and assumptions are same as the above lemma. Let $\mathrm{pr} : G \twoheadrightarrow G/Z(G)$ be the canonical projection. Then $\mathrm{pr}\circ f$ can be extended to a group homomorphism $\pi_1^{\mathrm{et}}(X_F\ , \bar{x}) \simeq \pi_1^{\mathrm{et}}(X_{\overline{F}}\ , \bar{x}) \rtimes G_F \to G/Z(G)$.*

Proof. We write the image of $g \in G$ in $G/Z(G)$ by $\bar{g}$. Since $\bar{g}_\epsilon\bar{g}_\tau = \bar{g}_{\epsilon\tau}$, the map $\tilde{f}((\tau,\beta)) := \bar{f}(\tau)\bar{g}_\beta$ is a group homomorphism. Indeed, we have the following equation:

$$\begin{aligned}
\tilde{f}((\tau,\beta)(\mu,\gamma)) &= \tilde{f}((\tau\mu^\beta,\beta\gamma)) = \bar{f}(\tau\mu^\beta)\bar{g}_{\beta\gamma} \\
&= \bar{f}(\tau)\bar{f}(\mu^\beta)\bar{g}_{\beta\gamma} = \bar{f}(\tau)\bar{g}_\beta\bar{f}(\mu)\bar{g}_\beta^{-1}\bar{g}_{\beta\gamma} \\
&= \bar{f}(\tau)\bar{g}_\beta\bar{f}(\mu)\bar{g}_\gamma = \tilde{f}((\tau,\beta))\tilde{f}((\mu,\gamma)).
\end{aligned}$$

□

Definition 2.9. *Let G be a finite group and $\mathcal{C} = (C_1, \dots, C_r)$ be an r-tuple of conjugacy classes of G. Put $S = S(\mathcal{C}) := \{\{C_1^n, \dots, C_r^n\} | (n, |G|) = 1\}$ and*

define an action $\kappa : G_{\mathbb{Q}} \to \mathrm{Aut}(S)$ *of* $G_{\mathbb{Q}}$ *on* S *as follows:*

$$\kappa(\epsilon)(\{C_1^n, \dots, C_r^n\}) := \{C_1^{n\chi(\epsilon)}, \dots, C_r^{n\chi(\epsilon)}\}.$$

where χ *is the cyclotomic character. We define an abelian extension* $\mathbb{Q}_{\mathcal{C}}$ *of* $\mathbb{Q}$ *so that* $\mathrm{Stab}_{G_{\mathbb{Q}}}(\{C_1, \dots, C_r\}) = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}_{\mathcal{C}})$.
We say that $\mathcal{C}$ *is rational if* $\mathbb{Q}_{\mathcal{C}} = \mathbb{Q}$.

Lemma 2.10. *([Vö, Lemma 3.16.]) Let* G *be a finite group and* $\mathcal{C} = (C_1, \dots, C_r)$ *be an* r*-tuple of conjugacy classes of* G*. Then, there exists a* $G_{\mathbb{Q}}$*-stable set of points* $\{x_i\}_{1 \le i \le r} \subset \mathbb{P}^1(\overline{\mathbb{Q}})$ *such that*

$$\{C_1, \dots, C_r\} \cong \{x_1, \dots, x_r\}$$

as $G_{\mathbb{Q}_{\mathcal{C}}}$*-sets. Here the action of* $G_{\mathbb{Q}_{\mathcal{C}}}$ *on* $\{C_1, \dots, C_r\}$ *is defined by* κ*.*

Now, we can prove Thompson's rigidity method .

Proof. (Proof of Proposition 1.4)
Let G be a finite group and $\mathcal{C} = (C_1, \dots, C_r)$ be an r-tuple of conjugacy classes of G. Put

$$\mathcal{E}^{\mathrm{in}}(\mathcal{C}) := \{(g_1, \dots, g_r) \in G^r \ | g_i \in C_i\}/\mathrm{Inn}G.$$

By Lemma 2.2, there exists an identification :

$$\mathcal{E}^{\mathrm{in}}(\mathcal{C}) \xrightarrow{\sim} \{f \in \mathrm{Surj}(\ \pi_1(X_{\overline{\mathbb{Q}}}, x), G) \mid f(\epsilon_i) \in C_i \ \}/ \ \mathrm{Inn}G \ .$$

Here we take $\{x_i\}$ so that

$$\{C_1, \dots, C_r\} \cong \{x_1, \dots, x_r\}$$

as $G_{\mathbb{Q}_{\mathcal{C}}}$-sets by Lemma 2.10. By Lemma 2.6, $G_{\mathbb{Q}_{\mathcal{C}}}$ acts on $\mathcal{E}^{\mathrm{in}}(\mathcal{C})$.

Assume that there exists an r-tuple of conjugacy classes $\mathcal{C}$ such that $|\,\mathcal{E}^{\mathrm{in}}(\mathcal{C})| = 1$ so $[g] \in \mathcal{E}^{\mathrm{in}}(\mathcal{C})$ is fixed by $G_{\mathbb{Q}_{\mathcal{C}}}$. Thus we have a 2-cocycle $c : G_{\mathbb{Q}_{\mathcal{C}}} \to Z(G)$ as the above. Since the cohomological dimension of $\mathbb{Q}^{\mathrm{ab}}$ is one, the restriction of c on $G_{\mathbb{Q}^{\mathrm{ab}}}$ is a 2-coboundary. Let $f : \pi_1^{\mathrm{et}}(X_{\overline{\mathbb{Q}}}\ , \bar{x}) \to G$ be a group homomorphism and $W \to \mathbb{P}^1_{\overline{\mathbb{Q}}}$ be a G-covering which corresponds to $[g]$. By applying Lemma 2.7 with $F = \mathbb{Q}^{\mathrm{ab}}$, f can be extended to a group homomorphism on $\pi_1^{\mathrm{et}}(X_{\mathbb{Q}^{\mathrm{ab}}}\ , \bar{x})$. According to Theorem-Definition 2.1, a G-covering $W \to \mathbb{P}^1_{\overline{\mathbb{Q}}}$ is defined over $\mathbb{Q}^{\mathrm{ab}}$ if and only if f can be extended to a group homomorphism $\pi_1^{\mathrm{et}}(X_{\mathbb{Q}^{\mathrm{ab}}}\ , x) \to G$.

Applying Lemma 2.8, the group homomorphism f can be extended to a group homomorphism $\tilde{f} : \pi_1^{\mathrm{et}}(X_{\mathbb{Q}_{\mathcal{C}}}\ , \bar{x}) \to G$. This completes the proof of Proposition 1.4. □

2.1.3 Example of configuration spaces

Let $\mathcal{U}_r(\mathbb{C}) := \{\{x_1, \ldots, x_r\} | x_i \in \mathbb{P}^1(\mathbb{C}), x_i \neq x_j \ if \ i \neq j\}$. The topological fundamental group of $\mathcal{U}_r(\mathbb{C})$ is the Artin's braid group B_r.

$B_r := \left\langle Q_i, 1 \leq i \leq r-1 \middle| \ Q_i \text{ satisfy the following eqations } \ (1),(2) \right\rangle$

$$Q_i Q_{i+1} Q_i = Q_{i+1} Q_i Q_{i+1}, [Q_i, Q_j] = 1 | i - j| \geq 2, \tag{1}$$

$$Q_1 \cdots Q_{r-2} Q_{r-1}^2 Q_{r-2} \cdots Q_1 = 1 \tag{2}$$

We define the action of $\pi_1^{\mathrm{top}}(\mathcal{U}_r(\mathbb{C}), u)$ on $\mathcal{E}_r^{\mathrm{in}}(G)$ by

$$Q_i[g_1, \ldots, g_r] := [g_1, \ldots, g_i g_{i+1} {g_i}^{-1}, g_i, \ldots, g_r] \ , \ [g_1, \ldots, g_r] \in \mathcal{E}^{\mathrm{in}}(G) \ .$$

This action is well-defined. By the definition of the fundamental group, there exists the finite etale covering $\mathcal{H}_r^{\mathrm{in}}(G) \to \mathcal{U}_{r\mathbb{C}}$ whose fiber at u is identified with $\mathcal{E}_r^{\mathrm{in}}(G)$. This is the classical Hurwitz space which are the moduli space of ramified G-coverings which are ramified at most r-points.

2.2 Hurwitz spaces

In this section, we construct Hurwitz spaces. Let F be a sub-field of $\mathbb{C}$. Consider the following diagram of F-schemes:

$$\begin{tikzcd} \mathcal{U} \arrow[r, "j"] \arrow[dr, "f"'] & \mathbb{P}_F^1 \times_F U \arrow[d, "\bar{f}"] \arrow[dl, phantom, "\circlearrowleft"] \arrow[dr, phantom, "\circlearrowleft"] & Y \arrow[l, "i"'] \arrow[dl, "\tilde{f}"] \\ & U & \end{tikzcd} \qquad (*)_{U,Y}$$

where Y is a relative normal crossing divisor of $\mathbb{P}_F^1 \times_F U$ over U and $\tilde{f}$ is a finite etale morphism, $\mathcal{U}$ is the complement of Y.

Let G be a finite group. By Theorem-Definition 2.1, a group homomorphism $\phi : \ \pi_1^{\mathrm{et}}(U, \bar{u}) \to \mathrm{Aut}(G)$ define a locally constant constructible sheaf $\mathcal{G}_\phi$ on U, where $\bar{u}$ is a geometric point of U.

The following well-known proposition is the key of our construction.

Proposition 2.11. *[SGA1, Exposé13 Theorem. 2.4] Let $\mathcal{G}$ be a locally constant constructible group sheaf on $\mathcal{U}_{\mathrm{et}}$. Then, $R^1 f_* \mathcal{G}$ is a locally constant constructible sheaf on U_{et}. Moreover $R^1 f_* \mathcal{G}$ is compatible with arbitrary base change by $U' \to U$.*

According to the above proposition, $R^1 f_* f^* \mathcal{G}_\phi$ is a locally constant constructible sheaf whose fiber is isomorphic to

$$\mathrm{H}^1(\mathbb{P}_{\overline{F}}^1 \setminus \{x_1, \ldots, x_r\}, (\mathcal{G}_\phi)_{\bar{u}}) = \mathrm{Hom}(\pi_1^{\mathrm{et}}(\mathbb{P}_{\overline{F}}^1 \setminus \{x_1, \ldots, x_r\}), G)/\mathrm{Inn}G.$$

We describe the action of $\pi_1^{\mathrm{et}}(U,\bar{u})$ on the fiber of $R^1 f_* f^* \mathcal{G}_\phi$ at $\bar{u}$.Assume that U has an F-rational point v, and we fix the isomorphism $\pi_1^{\mathrm{et}}(U,\bar{u}) \cong \pi_1^{\mathrm{et}}(U_{\overline{F}},\bar{u}) \rtimes G_F$ which is induced by $v \to U$.

The Action of G_F First, we determine the action of G_F on the fiber of $R^1 f_* f^* \mathcal{G}_\phi$ at $\bar{u}$. According to Proposition 4.12, we may assume that $U = $ Spec(F) . By definition, the sheaf $R^1 f_* f^* \mathcal{G}_\phi$ is the sheafification of the presheaf :

$$L/F \mapsto \mathrm{H}^1(\mathbb{P}_L \setminus \{x_1,\dots,x_r\}, G^{\phi(G_L)}).$$

Here L is an F-algebra and $G^{\phi(G_L)}$ is the fixed part of G by $\phi(G_L)$ the absolute Galois group of L.
The transformation of an F-algebra homomorphism $K \to L$ by the above presheaf

$$(K \to L/F) \mapsto \mathrm{H}^1(\mathbb{P}^1_K \setminus \{x_1,\dots x_r\}, G^{\phi(G_K)}) \to \mathrm{H}^1(\mathbb{P}^1_L \setminus \{x_1,\dots,x_r\}, G^{\phi(G_L)})$$

is decomposed as the following diagram:

$$\begin{tikzcd}
\mathrm{H}^1(\mathbb{P}^1_K \setminus \{x_1,\dots,x_r\}, G^{\phi(G_K)}) \arrow[r] \arrow[dr, "p"] & \mathrm{H}^1(\mathbb{P}^1_L \setminus \{x_1,\dots,x_r\}, G^{\phi(G_L)}) \\
\arrow[ur, phantom, "\circlearrowleft"] & \mathrm{H}^1(\mathbb{P}^1_L \setminus \{x_1,\dots,x_r\}, G^{\phi(G_K)}) \arrow[u, "\alpha"']
\end{tikzcd}$$

where p is the pullback of torsors by

$$\mathbb{P}^1_L \setminus \{x_1,\dots,x_r\} \longrightarrow \mathbb{P}^1_K \setminus \{x_1,\dots,x_r\}$$

and α is the map which is induced by a canonical morphism

$$G^{\phi(G_K)} \to G^{\phi(G_L)} .$$

Hence the action of $\beta \in G_F$ is decomposed as follows:

$$\begin{tikzcd}
\mathrm{H}^1(\mathbb{P}^1_{\overline{F}} \setminus \{x_1,\dots,x_r\}, G) \arrow[r] \arrow[dr, "\beta^*"] & \mathrm{H}^1(\mathbb{P}^1_{\overline{F}} \setminus \{x_1,\dots,x_r\}, G) \\
\arrow[ur, phantom, "\circlearrowleft"] & \mathrm{H}^1(\mathbb{P}^1_{\overline{F}} \setminus \{x_1,\dots,x_r\}, G) \arrow[u, "\phi(\beta)"]
\end{tikzcd}$$

where β^* is the pullback of torsors by

$$\beta : \mathbb{P}^1_{\overline{F}} \setminus \{x_1,\dots,x_r\} \longrightarrow \mathbb{P}^1_{\overline{F}} \setminus \{x_1,\dots,x_r\}$$

and $\phi(\beta)$ is the morphism induced by $\phi(\beta) \in \mathrm{Aut}(G)$ and $\overline{F}$ is the algebraic closure of F.

We conclude the following proposition:

Proposition 2.12. *Let $\phi : G_F \to \mathrm{Aut}(G)$ be a group homomorphism and $\mathcal{G} = \mathcal{G}_\phi$ be the locally constant constructible sheaf on $\mathrm{Spec}(F)_{\mathrm{et}}$ which is defined by ϕ. Let*

$$f : \mathbb{P}^1_F \setminus \{x_1, \dots, x_r\} \to \mathrm{Spec}(F)\ ,\ x_1, \dots, x_r \in \mathbb{P}^1(F)$$

be the structure morphism. Then the subset $\mathrm{Surj}(\pi_1^{\mathrm{et}}(\mathbb{P}^1_{\overline{F}} \setminus \{x_1, \dots, x_r\}), G)/\mathrm{Inn}G$ of the fiber of $R^1 f_* f^* \mathcal{G}_\phi$ at $\bar{u}$ is a G_F-stable subset. Under the identification $\mathrm{Surj}(\pi_1^{\mathrm{et}}(\mathbb{P}^1_{\overline{F}} \setminus \{x_1, \dots, x_r\}), G)/\mathrm{Inn}G$ with the set $\mathcal{E}_r^{\mathrm{in}}(G)$ (cf. Lemma 2.2), the action of G_F on $\mathcal{E}_r^{\mathrm{in}}(G)$ is described as follows:

$$\beta[g_1, \dots, g_r] = \phi(\beta) \circ \varphi_\beta[g_1, \dots, g_r]\ \beta \in G_F\ ,\ [g_1, \dots, g_r] \in \mathcal{E}_r^{\mathrm{in}}(G).$$

Here $\varphi_\beta \in \mathrm{Aut}(\mathcal{E}_r^{\mathrm{in}}(G))$ is the automorphism which is induced by the outer action of G_F on $\pi_1^{\mathrm{et}}(\mathbb{P}^1_{\overline{F}} \setminus \{x_1, \dots, x_r\})$ which is induced by the fundamental exact sequence (cf. Lemma 2.5).

The Action of $\pi_1^{\mathrm{et}}(U_{\overline{F}}, \bar{u})$ Next, we determine the action of the geometric fundamental group of U on the fiber of $R^1 f_* f^* \mathcal{G}_\phi$ at $\bar{u}$. We recall the following proposition.

Proposition 2.13. *([Fu, Proposition 5.4.]) A functor*

$$\mathrm{SDiv}^r : (\mathrm{Sch})/\mathbb{Z} \to (\mathrm{Sets}) \quad , \mathrm{SDiv}^r(S) := \{\textit{Simple divisors of } \mathbb{P}^1_S\}$$

is represented by the r-configuration space $\mathcal{U}_r$ over $\mathbb{Z}$.

According to Proposition 2.13, any diagram $(*)_{U,Y}$ is the pullback of $(*)_{\mathcal{U}_r, D_r}$. In other words, there exists the unique morphism

$$h : U \to \mathcal{U}_r$$

such that

$$(*)_{Y,U} = h^*(*)_{\mathcal{U}_r, D_r}$$

where D_r is the universal simple divisor which is defined by the following equation:

$$D_r := \{t^r - S_1 + \dots + (-1)^r S_r = 0\}$$

where S_i is the i-th elementary symmetric polynomial of a parameter system of $\mathcal{U}_r$ and t is a parameter of $\mathbb{P}^1_{\overline{F}}$. Thus, the action of $\pi_1(U_{\overline{\mathbb{Q}}}, \bar{u}))$ on the fiber of $R^1 f_* f^* \mathcal{G}_\phi$ at $\bar{u}$ factors through $h_* : \pi_1(U_{\overline{\mathbb{Q}}}, \bar{u}) \to \pi_1(\mathcal{U}_r, h(\bar{u}))$.

We recall the decription of the geometric fundamental group of $\mathcal{U}_r$(cf. [M-M, Section3.1.]). Let $u = \{u_1, \dots u_r\}$ be a point of $\mathcal{U}_r(\mathbb{C})$ and assume that $u_i \neq \infty$

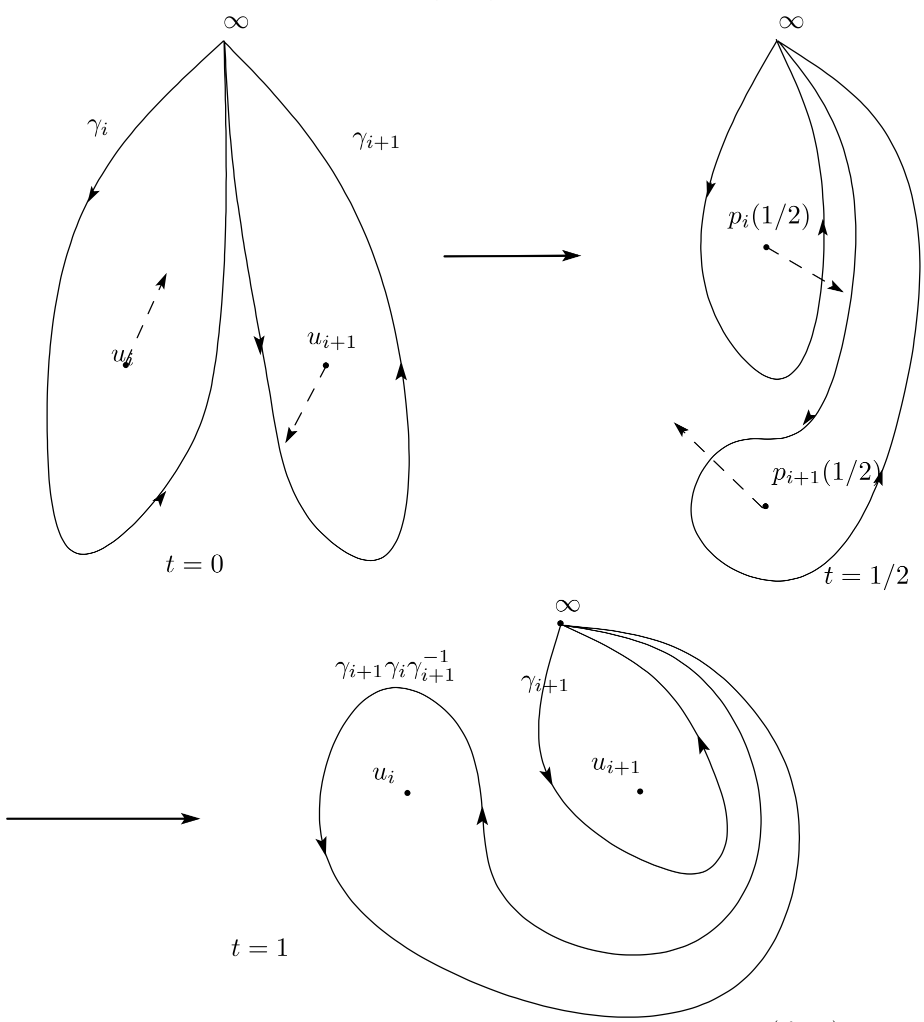
for all i and $u_j \notin \{w \in \mathbb{C} |\ |w - \frac{(u_i - u_{i+1})}{2}| \leq \frac{|(u_i - u_{i+1})|}{2}\}$ for $j \neq i, i+1$. Let $p_i : [0,1] \to \mathcal{U}_r(\mathbb{C})$, $1 \leq i \leq r-1$ be the loop which is defined as follows:

$$p_i(t) := \{u_1, \dots \frac{(u_i - u_{i+1})}{2}(\exp(\pi i t)+1), \frac{(u_i - u_{i+1})}{2}(\exp(-\pi i t)+1), u_{i+2}, \dots\}.$$

Then, the set of homotopy classes of $\{p_i\}_{i=1}^{r-1}$ generates $\pi_1^{\text{top}}(\mathcal{U}_r(\mathbb{C}), u)$. Moreover, there exists an isomorphism of groups:

$$B_r \xrightarrow{\sim} \pi_1^{\text{top}}(\mathcal{U}_r(\mathbb{C}), u)\ ,\ Q_i \mapsto [p_i]$$

where $\{Q_i\}_i$ the set of the generators of B_r which is defined in Section 2.1.3. The etale fundamental group of $\mathcal{U}_{r\overline{\mathbb{Q}}}$ acts on the fiber of $R^1 f_* G$ at $\bar{u}$ by permutation of the ramification points of torsors (fig 1).



$(fig1)$

Thus we conclude that $Q_i[g_1, \ldots, g_r] = [g_1, \ldots, g_i g_{i+1} {g_i}^{-1}, g_i, \ldots, g_r]$ for $[g_1, \ldots, g_r] \in \mathcal{E}_r^{\mathrm{in}}(G)$. This action coincides with the action defined in Section 2.1.3.

Proposition 2.14. *Let $(*)_{Y,U}$ be a diagram same as the diagram beginning of 2.2 and $\bar{u}$ be a geometric point of U. Let $\phi : \pi_1^{\mathrm{et}}(U_{\overline{F}}, \bar{u}) \to \mathrm{Aut}(G)$ be a group homomorphism and $\mathcal{G}_\phi$ be the locally constant constructible sheaf on U which is defined by ϕ. Then the subset $\mathrm{Surj}(\pi_1^{\mathrm{et}}(\mathbb{P}^1_{\overline{F}} \setminus \{x_1, \ldots, x_r\}), G)/\mathrm{Inn}G$ of the fiber of $R^1 f_* f^* \mathcal{G}_\phi$ at $\bar{u}$ is a $\pi_1^{\mathrm{et}}(U_{\overline{F}}, \bar{u})$-stable subset. Under the identification $\mathrm{Surj}(\pi_1^{\mathrm{et}}(\mathbb{P}^1_{\overline{F}} \setminus \{x_1, \ldots, x_r\}), G)/\mathrm{Inn}G$ with $\mathcal{E}_r^{\mathrm{in}}(G)$ (cf. Lemma 2.2), the action of $\pi_1^{\mathrm{et}}(U_{\overline{F}}, \bar{u})$ on $\mathcal{E}_r^{\mathrm{in}}(G)$ is described as follows:*

$$\sigma[g_1, \ldots, g_r] = h_*(\sigma)[\phi(\sigma)(g_1), \ldots, \phi(\sigma)(g_r)] \ , \ \sigma \in \pi_1^{\mathrm{et}}(U_{\overline{F}}, \bar{u}).$$

Here, $h : U \to \mathcal{U}_r$ is the unique morphism which satisfies $h^*(*)_{\mathcal{U}_r, D_r} = (*)_{U,Y}$ and the action of $\pi_1^{\mathrm{et}}(\mathcal{U}_{r\overline{F}}, \bar{u})$ on $\mathcal{E}_r^{\mathrm{in}}(G)$ is the action which is defined in Section 2.1.3.

Corollary 2.15. *Let F be a subfield of $\mathbb{C}$ and U be a connected locally Noetherian F-scheme. Let $(*)_{U,Y}$ be the diagram of F-schemes which is defined as follows:*

$$\begin{tikzcd}
\mathcal{U} := (\mathbb{P}^1_F \times_F U) \setminus Y \arrow[r, "j"] \arrow[drr, "f"', bend right=0] & & \mathbb{P}^1_F \times_F U \arrow[d, "\bar{f}"] \arrow[dl, phantom, "\circlearrowleft"] \arrow[dr, phantom, "\circlearrowright"] & & Y \arrow[ll, "i"'] \arrow[dll, "\tilde{f}"] \\
& & U & &
\end{tikzcd} \qquad (*)_{U,Y}$$

where Y is a relative normal crossing divisor of $\mathbb{P}^1_F \times_F U \to U$ which is finite etale over U. Let

$$\phi : \pi_1^{\mathrm{et}}(U, \bar{u}) \longrightarrow \mathrm{Aut}(G) \ , \bar{u} \in U(\overline{\mathbb{Q}})$$

be a group homomorphism and $\mathcal{G}_\phi$ be the locally constant constructible sheaf which is defined by ϕ. Then the subset

$$\mathrm{Surj}(\pi_1^{\mathrm{et}}(f^{-1}(\bar{u})), G)/\mathrm{Inn}G \subset \mathrm{Hom}(\pi_1^{\mathrm{et}}(f^{-1}(\bar{u})), G)/\mathrm{Inn}G = (R^1 f_* f^* \, \mathcal{G}_\phi)_{\bar{u}}$$

is stable by the action of $\pi_1^{\mathrm{et}}(U, \bar{u})$. Here we identify the fiber of $R^1 f_* f^* \, \mathcal{G}_\phi$ at $\bar{u}$ with $\mathrm{Hom}(\pi_1^{\mathrm{et}}(f^{-1}(\bar{u})), G)/\mathrm{Inn}G$ by using Lemma 2.2.

Proof. This is an elementary consequence of Proposition 2.14 and 2.18. ∎

Now we define the Hurwitz space attached to a given diagram and a given group homomorphism.

Definition 2.16. *Let F be a sub-field of $\mathbb{C}$ and U be connected locally Noetherian F-scheme. Let $(*)_{U,Y}$ be the diagram of F-schemes which is defined as follows:*

$$
\begin{tikzcd}
\mathcal{U} := (\mathbb{P}^1_F \times_F U) \setminus Y \arrow[r, "j"] \arrow[dr, "f"'] \arrow[dr, phantom, shift left=4, "\circlearrowleft"] & \mathbb{P}^1_F \times_F U \arrow[d, "\bar{f}"] \arrow[d, phantom, shift left=6, "\circlearrowleft"] & Y \arrow[l, "i"'] \arrow[dl, "\tilde{f}"] \\
& U &
\end{tikzcd}
\qquad (*)_{U,Y}
$$

where Y is a relative normal crossing divisor of $\mathbb{P}^1_F \times_F U \to U$ which is finite etale over U. Let

$$\phi : \pi_1^{\text{et}}(U, \bar{u}) \longrightarrow \text{Aut}(G) \ , \bar{u} \in U(\overline{\mathbb{Q}})$$

be a group homomorphism and $\mathcal{G}_\phi$ be the locally constant constructible sheaf which is defined by ϕ.
(1) Let S be a subset of $(R^1 f_* f^* \mathcal{G}_\phi)_{\bar{u}} = \text{Hom}(\pi_1^{\text{et}}(f^{-1}(\bar{u})), G)/\text{Inn}G$ which is stable under the action of $\pi_1^{\text{et}}(U, \bar{u})$. We define the subsheaf $\mathcal{H}^{\text{in}}(S)$ of $R^1 f_* f^* \mathcal{G}_\phi$ as the locally constant constructible sheaf on U_{et} whose fiber is isomorphic to S as $\pi_1^{\text{et}}(U, \bar{u})$-sets(cf. Theorem-Definition 2.1). We regard $\mathcal{H}^{\text{in}}(S)$ as a scheme which is finite etale over U.
(2) We denote the finite etale U-scheme $\mathcal{H}^{\text{in}}(\text{Surj}(\pi_1^{\text{et}}(f^{-1}(\bar{u})), G)/\text{Inn}G)$ by $\mathcal{H}^{\text{in}}(U, Y, \phi)$(cf. Corollary 2.15). We call $\mathcal{H}^{\text{in}}(U, Y, \phi)$ the Hurwitz space attached to $(*)_{U,Y}, \phi$.

Example 2.17. *The finite etale scheme $\mathcal{H}^{\text{in}}(\mathcal{U}_r, D_r, \text{triv})$ over $\mathcal{U}_r$ is the Hurwitz space which is defined by Fried and Völklein (cf.[Fr-Vö]). This is the moduli space of G-covering of $\mathbb{P}^1_{\mathbb{C}}$ which is ramified at most r-points. Here* $\text{triv} : \pi_1^{\text{et}}(\mathcal{U}_r, \bar{u}) \to \text{Aut}(G)$ *is the trivial group homomorphism.*

Let $\varphi : \mathcal{H}^{\text{in}}(\mathcal{U}_r, D_r, \text{triv}) \to \mathcal{U}_r$ be the structure morphism of $\mathcal{H}^{\text{in}}(\mathcal{U}_r, D_r, \text{triv})$. Let $u = \{x_1, \ldots, x_r\}$ be a $\overline{\mathbb{Q}}$-point of $\mathcal{U}_r$, then the fiber of φ at u is identified with $\text{Surj}(\pi_1(\mathbb{P}^1_{\overline{\mathbb{Q}}} \setminus u), G)/\text{Inn}G$. The action of the fundamental group of $\mathcal{U}_{r\overline{\mathbb{Q}}}$ on $\varphi^{-1}(u)$ is coincide with the example in Section 2.1.3.

Proposition 2.18. *[Fr-Vö, Theorem 1]Let G be a finite group.*
(1) Let L be an extension of $\mathbb{Q}$. Suppose that the center of G is trivial. Then, there exists a geometrically connected G covering of $\mathbb{P}^1_L$ which is ramified at most r-points if and only if $\mathcal{H}^{\text{in}}(\mathcal{U}_r, D, \text{triv})(L)$ is not empty.
(2) Let L be an extension of $\mathbb{Q}$ whose absolute Galois group G_L has cohomlogical dimension≤ 1. Then, the same equivalence as that of (2) holds without any assumption of G.

The proof of Proposition 2.18 is almost same as the proof of the following theorem.

We generalize Proposition 2.18 as follows.

Theorem 2.19. *Let F be a sub-field of $\mathbb{C}$ and U be an algebraic variety over F. Let G be a finite group and L be an extension of F. Let $\phi : \pi_1(U, \bar{v}) \to \mathrm{Aut}(G)$ be a group homomorphism. Assume that U has an F-valued point v.*
(1) Assume that $\mathcal{H}^{\mathrm{in}}(U, Y, \mathcal{G}_\phi)(L)$ is not empty. Let $w \in \mathcal{H}^{\mathrm{in}}(U, Y, \mathcal{G}_\phi)(L)$ and $[g] \in \mathcal{E}_r^{\mathrm{in}}(G)$ be the element which corresponds to w by identification of Lemma 2.2. If the subgroup $\phi \circ i_v(G_L)$ of $\mathrm{Aut}(G)$ fixes $[g]$, then there exists a geometrically connected $G/Z(G)$-covering of $\mathbb{P}^1_L$ which is ramified at most r-points. Here $i_v : G_F \to \pi_1^{\mathrm{et}}(U, \bar{v})$ is the group homomorphism which is induced by v, and $\mathcal{G}_\phi$ be the locally constant constructible sheaf which is defined by ϕ.
(2) Moreover if the cohomoloigical dimension of the absolute Galois group G_L of L is less than 1, then there exists a geometrically connected G-covering of $\mathbb{P}^1_L$ which is ramified at most r-points.

Proof. (1) Let $u \in U(L)$ be the image of w. Since the formalism $R^1 f_* f^* \mathcal{G}_\phi$ is compatible with arbitrary base-change by $U' \to U$, we have an isomorphism $\mathcal{H}^{\mathrm{in}}(U, Y, \mathcal{G}_\phi) \times_U \bar{w} \xrightarrow{\sim} \mathcal{H}^{\mathrm{in}}(f^{-1}(\bar{w}), \tilde{f}^{-1}(\bar{w}), \mathcal{G}_{\phi_{\bar{w}}}) = \mathrm{Surj}(f^{-1}(\bar{w}), G)/\mathrm{Inn}(G)$. Here $\bar{w}$ is a geometric point which lies w. We may assume that $\mathcal{G}_\phi$ is a constant sheaf.

Let $[f] \in \mathrm{Surj}(\pi_1^{\mathrm{et}}(f^{-1}(\bar{w})), G)/\mathrm{Inn}(G)$ be the element which corresponds to w and $[g]$. Since $\phi \circ i_v(G_L)$ fixes $[g]$, we can construct a group homomorphism $\tilde{f} : \pi_1^{\mathrm{et}}(f^{-1}(w)) \to G/Z(G)$ which is an extension of f exactly same way as Lemma 2.8. (2) We define $c \in H^2(G_L, Z(G))$ same as the proof of Proposition 1.4. Since the cohomological dimension of L less than 2, this cocycle is trivial. Then we can construct a group homomorphism $\tilde{f} : \pi_1^{\mathrm{et}}(f^{-1}(w)) \to G$ which is an extension of f exactly same way as Lemma 2.7. This completes the proof of the theorem. □

Corollary 2.20. *Let G, F, L, ϕ be same as (1) of Theorem 2.19. Assume that $\phi \circ i_v(G_L) \subset \mathrm{Inn}(G)$. If $\mathcal{H}^{\mathrm{in}}(U, Y, \mathcal{G}_\phi)(L)$ is not empty, then there exists a geometrically connected $G/Z(G)$-covering of $\mathbb{P}^1_L$ which is ramified at most r-points.*

Proof. This is a special case of (1) of Theorem 2.19. □

Remark 2.21. *We can treat more general situation. Consider the following diagram.*

$$\begin{tikzcd}
X \arrow[r, "j"] \arrow[dr, "f"'] & \overline{X} \arrow[d, "\bar{f}"] & Y \arrow[l, "i"'] \arrow[dl, "\tilde{f}"] \\
& U &
\end{tikzcd} \qquad (*)_{U,Y}$$

where $f : X \to U$ is smooth and $\tilde{f} : \overline{X} \to U$ is proper smooth, Y is a relative normal crossing divisor over U. Then, we can define $\mathcal{H}^{\mathrm{in}}(U, Y, \mathrm{triv})$ as the above.

If G has trivial center, then $\mathcal{H}^{\mathrm{in}}(U, Y, \mathrm{triv})(F)$ can be identified with the set of geometrically connected G-coverings of $\overline{X}_u$, $u \in U(F)$ whose ramification points are contained in Y_u.

That has meaning to consider a family of rational varieties or punctured elliptic curves. Because these varieties satisfy property Hilbertian (see [Se, Chapter 2]).

3 First Main Theorem and an Application

In Section 3 and 4, we show some applications of Theorem 2.19. We fix the following notation.

- $\mathcal{E}_r^{\mathrm{in}}(G) := \{\ (g_1, \ldots, g_r) \in G^r \mid g_1 \ldots g_r = 1\ ,\ \langle g_1, \ldots, g_r \rangle = G\ \}/\mathrm{Inn}G$ for a finite group G.
- $\mathcal{E}^{\mathrm{in}}(\mathcal{C}) := \{\ [g_1, \ldots, g_r] \in \mathcal{E}^{\mathrm{in}}(G) \mid g_i \in \mathcal{C}_i\}$ for a finite group G and an r-tuple of conjugacy classes $\mathcal{C} = (\mathcal{C}_1, \ldots, \mathcal{C}_{\mathrm{r}})$ of G.
- $\mathrm{Aut}_{\mathcal{C}}(G) := \{f \in \mathrm{Aut}(G) \mid f(\mathcal{C}_i) = \mathcal{C}_i\ \ 1 \leq \forall i \leq r\}$ for a finite group G and an r-tuple of conjugacy classes $\mathcal{C} = (\mathcal{C}_1, \ldots, \mathcal{C}_{\mathrm{r}})$ of G.

3.1 A Generalization of the Rigidity Method

In this subsection, we generalize Proposition 1.4(Thompson's rigidity method).

Lemma 3.1. *Let k be a field of characteristic 0 and X be a connected proper smooth curve over k. If there exists finite flat morphism $f : X \to \mathbb{P}^1_k$ which is ramified at $x, y \in \mathbb{P}^1(k)$, then X is isomorphic to $\mathbb{P}^1_k$ over k.*

Proof. By Riemann-Hurwitz formula([Liu, Chapter 7,Thm.4.16.]), we have the following equation:

$$-2 = -2\deg(f) + \Sigma_{z \in f^{-1}(x)}(e_z - 1)[k(z) : k] + \Sigma_{z \in f^{-1}(y)}(e_z - 1)[k(z) : k]$$

where e_z is the ramification index of $\mathcal{O}_{\mathbb{P}^1_k, f(z)} \to \mathcal{O}_{X,z}$ and $k(z)$ is the residue field of z. Since $\Sigma_{z \in f^{-1}(x)} e_z[k(z) : k] = \Sigma_{z \in f^{-1}(y)} e_z[k(z) : k] = \deg(f)$, we have

$$\Sigma_{z \in f^{-1}(x)}[k(z) : k] + \Sigma_{z \in f^{-1}(y)}[k(z) : k] = 2.$$

Because of f is surjective, there exists k-rational points of X. So X is isomorphic to projective line over k([Liu, Chapter 7,Prop.4.1.]). ∎

Theorem 3.2. *Let G be a finite group and r be a positive integer. Assume that there exists an r-tuple of conjugacy classes $\mathcal{C} = (C_1, \ldots, C_r)$ of G which satisfy the following conditions:*

(a) There exists a subgroup $H \subset \mathrm{Aut}_{\mathcal{C}}(G)$ which acts on $\mathcal{E}^{\mathrm{in}}(\mathcal{C})$ transitively.
(b) The group H is an abelian group or a dihedral group D_n.
Then G is regular over $\mathbb{Q}^{\mathrm{ab}}$.

Proof. If H is a cyclic group or dihedral group D_n, there exists a faithful group representation $\rho : H \longrightarrow \mathrm{Aut}(\mathbb{P}^1_{\mathbb{Q}^{\mathrm{ab}}})$. This group representation defines a geometrically connected H-covering $h : \mathbb{P}^1_{\mathbb{Q}^{\mathrm{ab}}} \to \mathbb{P}^1_{\mathbb{Q}^{\mathrm{ab}}}/\rho(H) \cong \mathbb{P}^1_{\mathbb{Q}^{\mathrm{ab}}}$. Put $U := \mathbb{P}^1_{\mathbb{Q}^{\mathrm{ab}}} \setminus \{\text{ramification points of } h\}$.

By the definition of U, the Galois group of

$$\mathbb{P}^1_{\overline{\mathbb{Q}}} \setminus h^{-1}(\{\text{ram. pts. of } h\}) \to \mathbb{P}^1_{\mathbb{Q}^{\mathrm{ab}}} \setminus h^{-1}(\{\text{ram. pts. of } h\}) \xrightarrow{h} U$$

is isomorphic to $H \times G_{\mathbb{Q}^{\mathrm{ab}}}$, there exists a representation

$$\phi : \pi_1^{\mathrm{et}}(U) \twoheadrightarrow H \subset \mathrm{Aut}_{\mathcal{C}}(G)$$

such that $\phi(\mathrm{G}_{\mathbb{Q}^{\mathrm{ab}}}) = 1$. Let $\mathcal{H}^{\mathrm{in}}(U, \{x_1, \ldots, x_r\} \times U, \phi)$ be the Hurwitz space attached to the following diagram and ϕ:

$$\begin{tikzcd}
(\mathbb{P}^1_{\mathbb{Q}^{\mathrm{ab}}} \setminus \{x_1, \ldots, x_r\}) \times U \arrow[r, "j"] \arrow[dr, "f"'] & \mathbb{P}^1_{\mathbb{Q}^{\mathrm{ab}}} \times U \arrow[d, "\bar{f}"] & \{x_1 \ldots, x_r\} \times U \arrow[l, "i"'] \arrow[dl, "\tilde{f}"] & (*)_{U,\{x_1,\ldots,x_r\}\times U} \\
 & U & &
\end{tikzcd}$$

where $x_i \in \mathbb{P}^1(\mathbb{Q})$.
Since the action of H on S is transitive, the sub-scheme

$$\mathcal{H}^{\mathrm{in}}(\mathcal{E}^{\mathrm{in}}(\mathcal{C})) \subset \mathcal{H}^{\mathrm{in}}(U, \{x_1, \ldots, x_r\} \times U, \phi)$$

which corresponds the $G_{\mathbb{Q}^{\mathrm{ab}}}$-stable subset $\mathcal{E}^{\mathrm{in}}(\mathcal{C})$ of $\mathcal{E}^{\mathrm{in}}_r(G)$ (cf. Definition 2.16) is geometrically connected. There exists a commutative diagram

$$\begin{tikzcd}
\mathbb{P}^1_{\overline{\mathbb{Q}}} \setminus h^{-1}(\text{ramification points}) \arrow[rr] \arrow[dr, "h"'] & & \mathcal{H}^{\mathrm{in}}(\mathcal{E}^{\mathrm{in}}(\mathcal{C}))_{\overline{\mathbb{Q}}} \arrow[dl] \\
 & U_{\overline{\mathbb{Q}}}. &
\end{tikzcd}$$

Here any morphisms are finite etale. Therefore, the smooth compactification X of $\mathcal{H}^{\mathrm{in}}(\mathcal{E}^{\mathrm{in}}(\mathcal{C}))$ is a projective line over $\mathbb{Q}^{\mathrm{ab}}$ or a conic over $\mathbb{Q}^{\mathrm{ab}}$. There exists the decomposition $\mathcal{H}^{\mathrm{in}}(\mathcal{E}^{\mathrm{in}}(\mathcal{C})) \xrightarrow{u} Y \xrightarrow{v} U$ whish corresponds to the decomposition

of $\pi_1^{\mathrm{et}}(U)$-sets $\mathcal{E}^{\mathrm{in}}(\mathcal{C}) \to \mathcal{E}^{\mathrm{in}}(\mathcal{C})/C_n \to *$. Here C_n is a cyclic group of order n and $*$ is the trivial $\pi_1^{\mathrm{et}}(U)$ set. Since every ramification point of h is a $\mathbb{Q}$-valued point, morphisms u, v satisfy the assumption of Lemma 3.1. Thus X is a projective line over $\mathbb{Q}^{\mathrm{ab}}$. In particular we have $\mathcal{H}^{\mathrm{in}}(\mathcal{E}^{\mathrm{in}}(\mathcal{C}))(\mathbb{Q}^{\mathrm{ab}}) \neq \emptyset$. By applying Corollary 2.20 for $L = K$ or $\mathbb{Q}^{\mathrm{ab}}$, $\mathcal{H}^{\mathrm{in}}(\mathcal{E}^{\mathrm{in}}(\mathcal{C}))$ and ϕ, we complete the proof of Theorem 3.2. If H is an abelian group, we take U a product of $\mathbb{A}^1_{\mathbb{Q}^{\mathrm{ab}}} \setminus \{0\}$ and proof is done in the same way. $\square$

Theorem 3.3. *Let G be a finite group and $\mathcal{C} = (C_1, \ldots, C_r)$ be an r-tuple of conjugacy classes of G. Assume that the triple $G, \mathcal{C}, H$ satisfy the condition (a) and (b) of Theorem 3.2.*
(1) The group $G/Z(G)$ is regular over $\mathbb{Q}_{\mathcal{C}}(\mu_m)$ where the positive integer m is defined as follows:

$$m := \begin{cases} \text{the exponent of } H & \text{if } H \text{ is abelian.} \\ n & \text{if } H = D_n. \end{cases}$$

(2) Moreover if the inclusion from H to $\mathrm{Aut}_{\mathcal{C}}(G)$ can be extended to an inclusion from $(\mathbb{Z}/m\mathbb{Z})^\times \ltimes H$ to $\mathrm{Aut}_{\mathcal{C}}(G)$ and if the action of $(\mathbb{Z}/m\mathbb{Z})^\times$ on $\mathcal{E}^{\mathrm{in}}(\mathcal{C})$ is trivial, then $G/Z(G)$ is regular over $\mathbb{Q}_{\mathcal{C}}$.

Proof. (1)We prove only the case that H is isomorphic to D_n or $\mathbb{Z}/n\mathbb{Z}$. Let $\rho : H \longrightarrow \mathrm{Aut}(\mathbb{P}^1_{\mathbb{Q}^{\mathrm{ab}}})$ be a faithful representation as Theorem 2. This action of H on $\mathbb{P}^1_{\mathbb{Q}^{\mathrm{ab}}}$ is defined over $\mathbb{P}^1_{\mathbb{Q}(\mu_n)}$ where μ_n is the group which consists n-th roots of unity. Take a $G_{\mathbb{Q}_{\mathcal{C}}}$-stable subset $\{x_1, \ldots, x_r\} \subset \mathbb{P}^1_{\overline{\mathbb{Q}}}$ such that

$$\{x_1, \ldots, x_r\} \cong \{C_1, \ldots, C_r\}$$

as $G_{\mathbb{Q}_{\mathcal{C}}}$-sets(Lemma 2.10). Thus the Hurwitz space $\mathcal{H}^{\mathrm{in}}(U, \{x_1, \ldots, x_r\} \times U, \phi)$, which is defined in the proof of Theorem 3.2, is defined over $\mathbb{Q}(\mu_n)$.
By the definition of $\mathbb{Q}_{\mathcal{C}}$, the connected component $\mathcal{H}^{\mathrm{in}}(\mathcal{E}^{\mathrm{in}}(\mathcal{C}))$ of the Hurwitz space $\mathcal{H}^{\mathrm{in}}(U, \{x_1, \ldots, x_r\} \times U, \phi)$ is defined over $\mathbb{Q}_{\mathcal{C}}(\mu_n)$.

The arithmetic genus of the smooth compactification X of $\mathcal{H}^{\mathrm{in}}(\mathcal{E}^{\mathrm{in}}(\mathcal{C}))$ equal to the geometric genus and it is equal to 0 (see [Liu, Prop4.1.]). Thus, the smooth compactification X of $\mathcal{H}^{\mathrm{in}}(\mathcal{E}^{\mathrm{in}}(\mathcal{C}))$ is isomorphic to $\mathbb{P}^1_{\mathbb{Q}_{\mathcal{C}}(\mu_n)}$ or a conic over $\mathbb{Q}_{\mathcal{C}}(\mu_n)$ (see [Liu, Cor 3.11]). After the same argument in the proof of Theorem 3.2, we conclude that X is a projective line over $\mathbb{Q}_{\mathcal{C}}(\mu_n)$. In particular $\mathcal{H}^{\mathrm{in}}(\mathcal{E}^{\mathrm{in}}(\mathcal{C}))(\mathbb{Q}_{\mathcal{C}}(\mu_n)) \neq \emptyset$, this completes the proof of (1) of Theorem 3.3.

(2) By the assumption of (2), the group homomorphism ϕ can be extended to a group homomorphism

$$\pi_1^{\mathrm{et}}(U') \twoheadrightarrow (\mathbb{Z}/n\mathbb{Z})^\times \ltimes H \to \mathrm{Aut}_{\mathcal{C}}(G)$$

where $U' := \mathbb{P}^1_{\mathbb{Q}} \setminus \{\text{ramification points of } h\}$. Then the subset of the Hurwitz space $\mathcal{H}^{\mathrm{in}}(\mathcal{E}^{\mathrm{in}}(\mathcal{C}))$ is defined over $\mathbb{Q}_{\mathcal{C}}$. After the same argument as above, we conclude that $\mathcal{H}^{\mathrm{in}}(\mathcal{E}^{\mathrm{in}}(\mathcal{C}))$ is a projective line over $\mathbb{Q}_{\mathcal{C}}$. In particular, we have $\mathcal{H}^{\mathrm{in}}(\mathcal{E}^{\mathrm{in}}(\mathcal{C}))(\mathbb{Q}_{\mathcal{C}}) \neq \emptyset$. This completes the proof of (2). $\square$

Theorem 3.4. *Let G be a finite group and $\mathcal{C}$ be an r-tuple of conjugacy classes of G. Assume that the triple $G, \mathcal{C}, H$ satisfy the condition (a) and (b) of Theorem 3.2 and $H \subset (\mathbb{Z}/2\mathbb{Z})^2 \rtimes S_2 = D_4$ and that the action of H on $\mathcal{E}^{\mathrm{in}}(\mathcal{C})$ factors through the canonical morphism $H \subset D_4 \twoheadrightarrow D_4/\langle(1,1)\rangle \cong (\mathbb{Z}/2\mathbb{Z})^2$. If the action of H can be extended to an action of D_4, then $G/Z(G)$ is regular over $\mathbb{Q}_{\mathcal{C}}$.*

Proof. Let ϕ be a group homomorphism

$$\phi : \pi_1((\mathbb{G}_{m,\mathbb{Q}})^2/S_2) \to \mathrm{Gal}(\mathbb{Q}(s,t)/\mathbb{Q}(u,v)) \cong (\mathbb{Z}/2\mathbb{Z})^2 \rtimes S_2 = D_4 \to \mathrm{Aut}(G)$$

where $u = s^2+t^2, v = s^2t^2$. By the assumption, ϕ factors through the surjection

$$\mathrm{Gal}(\mathbb{Q}(s,t)/\mathbb{Q}(u,v)) \twoheadrightarrow \mathrm{Gal}(\mathbb{Q}(s/t,st)/\mathbb{Q}(u,v)) = \mathrm{Gal}(\mathbb{Q}(\frac{s}{t},st)/\mathbb{Q}((\frac{s}{t})^2,(st)^2)).$$

Take a $G_{\mathbb{Q}_{\mathcal{C}}}$-stable subset $\{x_1,\dots,x_r\} \subset \mathbb{P}^1_{\mathbb{Q}}$ such that $\{x_1,\dots,x_r\} \cong \{C_1,\dots,C_r\}$ as $G_{\mathbb{Q}_{\mathcal{C}}}$-sets. The Hurwitz space $\mathcal{H}^{\mathrm{in}}((\mathbb{G}_{m,\mathbb{Q}})^2/S_2), \{x_1,\dots,x_r\} \times ((\mathbb{G}_{m,\mathbb{Q}})^2/S_2), \phi)$ is defined over $\mathbb{Q}_{\mathcal{C}}$.

If $H = D_4$, the connected component $\mathcal{H}^{\mathrm{in}}(\mathcal{C})$ of the above Hurwitz space $\mathcal{H}^{\mathrm{in}}((\mathbb{G}_{m,\mathbb{Q}})^2/S_2), \{x_1,\dots,x_r\} \times ((\mathbb{G}_{m,\mathbb{Q}})^2/S_2), \phi)$ is geometrically connected because the action of D_4 on $\mathcal{E}^{\mathrm{in}}(\mathcal{C})$ is transitive. According to the above remark, $\mathcal{H}^{\mathrm{in}}(\mathcal{C})$ is a product of double coverings of $\mathbb{G}_{m,\mathbb{Q}_{\mathcal{C}}}$. Thus $\mathcal{H}^{\mathrm{in}}(\mathcal{C})$ is a rational variety over $\mathbb{Q}_{\mathcal{C}}$ (Lemma 2.10). By applying Corollary 2.20, we have the conclusion of Theorem 3.4 in this case.

If $H = \mathbb{Z}/4\mathbb{Z} \subset D_4$, the connected component $\mathcal{H}^{\mathrm{in}}(\mathcal{E}^{\mathrm{in}}(\mathcal{C}) \cup \phi(\alpha)(\mathcal{E}^{\mathrm{in}}(\mathcal{C})))$ of $\mathcal{H}^{\mathrm{in}}((\mathbb{G}_{m,\mathbb{Q}})^2/S_2), \{x_1,\dots,x_r\} \times ((\mathbb{G}_{m,\mathbb{Q}})^2/S_2), \phi)$ which corresponds the $G_{\mathbb{Q}_{\mathcal{C}}}$-stable set $\mathcal{E}^{\mathrm{in}}(\mathcal{C}) \cup \phi(\alpha)(\mathcal{E}^{\mathrm{in}}(\mathcal{C}))$ of $\mathcal{E}^{\mathrm{in}}_r(G)$ (cf. Definition 2.16) is geometrically connected and isomorphic to a product of double coverings of $\mathbb{G}_{m,\mathbb{Q}_{\mathcal{C}}}$. Here α is an element of D_4 which is not contained by H. Thus $\mathcal{H}^{\mathrm{in}}(\mathcal{E}^{\mathrm{in}}(\mathcal{C}) \cup \phi(\alpha)(\mathcal{E}^{\mathrm{in}}(\mathcal{C})))$ is a rational variety over $\mathbb{Q}_{\mathcal{C}}$ (Lemma 2.10). By applying Corollary 2.20, we have the conclusion of Theorem 3.4 in the case $H = \mathbb{Z}/4\mathbb{Z}$.

If the exponent of H is equal to 2, we deduce the conclusion of this theorem by Theorem 3.3.

If $H = \{1\}$, we deduce the conclusion of the theorem by Proposition 1.4.

This completes the proof of the theorem. □

3.2 Group Theoretic Preliminaries

In this section, we recall some group theoretic lemmas needed later.

Definition 3.5. *Let K be a field. We say that an element $g \in GL_n(K)$ is perspectivities (resp. biperspectivities) if* $\mathrm{rk}(g-1) = 1$ *(resp.*$\mathrm{rk}(g-1) = 2$*).*
A semi-simple perspectivities is called a homology and an unipotent perspectivities is called transvection.

Lemma 3.6. *([W, Theorem 1.2.]) Let G be a primitive irreducible subgroup of $GL_n(\mathbb{F}_q)$, $n > 2$. If G contains a homology of order $m > 2$,then one of following*

holds:
(a) $SL_n(\mathbb{F}_{q_0}) \subset G \subset Z(G)GL_n(\mathbb{F}_{q_0}),\ \mathbb{F}_{q_0} \subset \mathbb{F}_q$ *and* $m \mid (q_0 - 1)$.
(b) $SU_n(\mathbb{F}_{q_0}) \subset G \subset Z(G)GU_n(\mathbb{F}_{q_0}),\ \mathbb{F}_{q_0{}^2} \subset \mathbb{F}_q$ *and* $m \mid (q_0 + 1)$.
(c) $SU_3(\mathbb{F}_2) \subset G \subset Z(G)GU_3(\mathbb{F}_2),\ m = 3,\ n = 3,\ p \neq 2,\ 3 \mid (q-1)$.
(d) $SU_4(\mathbb{F}_2) \subset G \subset Z(G)GU_4(\mathbb{F}_2),\ m = 3,\ n = 4,\ p \neq 2,\ 3 \mid (q-1)$.

The following lemmas are needed to prove the primitiveness of subgroup which are generated by a tuple of elements of $GL_n(\mathbb{F}_q)$.

Lemma 3.7. *([D-R, Lemma 6.6]) Let* $T = (T_1, \dots, T_r) \in GL_n(\mathbb{F}_q)^r$ *be an absolutely irreducible r-tuple such that* $\langle T \rangle := \langle T_1, \dots, T_r \rangle$ *is absolutely irreducible and* $\prod_{i=1}^{r} T_i$ *is a scalar. Put* $m := \sum_{i=1}^{r} \mathrm{rk}(T_i - 1)$*. Let* $x_i \in \mathbb{Z}_{>0}$ *be the maximal length of a Jordon block occurring in the Jordon decompositions of* T_i *which is not divisible by* p *and* $\oplus_{i=1}^{l} V_i$ *be a* $\langle T \rangle$*-invariant decomposition of* $\mathbb{F}_q^n$*. Let* $\phi : \langle T \rangle \to S_l$ *be the induced map. Then* $\phi(T_i) = 1$ *for* $\mathrm{rk}(T_i) < \dim(V_1)$ *and*

$$\dim(V_1) \geq \max\{\max_i\{x_i\},\ n - \frac{m}{2} + \frac{1}{2}(a + b)\}$$

where

$$a := \sum_{\substack{T_i:\ \textit{semi-simple} \\ rk(T_i - 1) < \dim V_1}} \mathrm{rk}(T_i - 1)$$

and

$$b := \sum_{T_i:\ unipotent} \Big(\sum_{\substack{\textit{Jordon blocks} \\ \textit{of } T_i}} \textit{length of Jordon blocks of } T_i \textit{ not divisible by } p \Big)\ .$$

Lemma 3.8. *([K-L, Lemma 2.10.1])Let* $G \subset GL_n(\mathbb{F}_q)$ *be an irreducible subgroup. Then* G *is absolutely irreducible if and only if the centralizer of* G *in* $GL_n(\mathbb{F}_q)$ *is* $\mathbb{F}_q^\times$*.*

We treat orthogonal group later, so recall some definitions and lemmas.

Definition 3.9. *([K-L, Section 2]) Let* K *be a field and* V *be a finite dimensional* K*-vector space. Let* Q *be a quadratic form on* V*.*
(1) A non-zero vector v *of* V *is singular if* $Q(v) = 0$*.*
(2) A subspace W *of* V *is totally singular if* $Q(w) = 0\ ,\ \forall w \in W$*.*
(3) Let $v \in V$ *be a non-singular vector. Then the reflection* r_v *with respect to* v *is an element of* $GL(V)$ *which is defined by* $r_v(x) := x - \frac{(x,v)}{Q(v)} v$ *where* $(x, v) := Q(x + v) - Q(x) - Q(v)$*.*

The following lemmas are used to prove rationality of some tuple of conjugacy classes.

Lemma 3.10. *([K-L, Proposition 2.5.2])Let K be a field and V be a finite dimensional K-vector space. Let Q be a quadratic form on V. Then maximal totally singular subspace is of dimension at most $\frac{1}{2}\dim(V)$.*

Corollary 3.11. *Let V be a finite dimensional $\mathbb{F}_q$-vector space and Q be a quadratic form of V. Let G be an orthogonal group with respect to Q. If $u \in G$ be an unipotent element such that $\mathrm{rk}(u-1) > \frac{1}{2}\dim V$, then the conjugacy class of $G \cap SL(V)$ which contains u is rational.*

Proof. The conjugacy class of G which contains u is rational ([D-R, Lemma 6.8]). Hence it is sufficient to prove that there exists a reflection of G which commutes with u. By applying Lemma 3.10, there exists $x \in V^{u=1}$ such that $Q(x)$ is non-zero. Then reflection r_x with respect to x commutes with u. Indeed, $Qr_xQ^{-1} = r_{Q(x)} = r_x$. $\square$

Lemma 3.12. *Let V, G be same as Corollary 3.11. Let $g \in G \cap SL(V)$ be a semi-simple biperspectivities of order 3. If $\dim V \geq 4$, then the conjugacy class of $G \cap SL(V)$ which contains g is rational.*

Proof. It is sufficient to prove that g and g^{-1} are conjugate in $G \cap SL(V)$. If $x, y \in V$ be eigen vectors of g, then the restriction of Q on $\langle x, y \rangle$ is non-degenerate. Since $\dim V \geq 4$, there exists a non-singular vector v such that $(v, x) = (v, y) = 0$. Therefore we have $[r_v, r_{x-y}] = [r_v, g] = 1$ and $r_v r_{x-y} g r_{x-y}^{-1} r_v^{-1} = r_{x-y} g r_{x-y}^{-1} = g^{-1}$. Since $r_v r_{x-y} \in G \cap SL(V)$, we obtain the conclusion of the lemma.

$\square$

3.3 Middle Convolution Functors

In this section, we recall definitions and basic properties of middle convolution functors given in [D-R]. Throughout this paper, we denote the free group of rank r by $\mathcal{F}_r$ and fix a set of generators $\{\sigma_1^{(r)}, \dots, \sigma_r^{(r)} \in \mathcal{F}_r\}$ of $\mathcal{F}_r$ for each positive integer r.

Definition 3.13. *Let r be a positive integer and K be a field. We denote the category of finite dimensional linear representations of $\mathcal{F}_r$ over K by $\mathrm{Rep}_K(\mathcal{F}_r)$. In other words, $\mathrm{Rep}_K(\mathcal{F}_r)$ is the category of pairs (V, ρ_V) of a finite dimensional K-vector space V and a group homomorphism $\rho_V : \mathcal{F}_r \to GL(V)$. We often denote (V, ρ_V) by V.*

We often identify an object of $(V\rho_V) \in \mathrm{Rep}_K(\mathcal{F}_r)$ with an r-tuple of elements $(\rho_V(\sigma_1), \dots, \rho_V(\sigma_r^{(r)}))$ of $GL(V)$.

Definition 3.14. *([D-R, Definition 2.2.])Let r be a positive integer. Let K be a field and (V, ρ_V) be an object of $\mathrm{Rep}_K(\mathcal{F}_r)$. For each $\lambda \in K^\times$, we define a functor $\mathrm{C}_\lambda^{(r)} : \mathrm{Rep}_K(\mathcal{F}_r) \to \mathrm{Rep}_K(\mathcal{F}_r)$ as follows:*

$$\mathrm{C}_\lambda^{(r)}((V, \rho_V)) := (V^r, \mathrm{C}_\lambda^{(r)}(\rho_V))$$

where

$$\mathrm{C}_\lambda^{(r)}(\rho_V)(\sigma_i^{(r)}) := \begin{pmatrix} \mathrm{Id}_V & O & \cdots\cdots\cdots\cdots & & & O \\ O & \ddots & \cdots\cdots\cdots\cdots & & & \vdots \\ X_1 - \mathrm{Id}_V & \dots & \lambda X_i & \lambda(X_{i+1} - \mathrm{Id}_V) & \dots & \lambda(X_r - \mathrm{Id}_V) \\ O & \cdots & O & \mathrm{Id}_V & \dots & O \\ \vdots & & \cdots\cdots\cdots & & \ddots & \vdots \\ O & \cdots\cdots\cdots\cdots & & & & \mathrm{Id}_V \end{pmatrix} \tag{3}$$

where $X_i := \rho_V(\sigma_i^{(r)})$.

Lemma 3.15. *([D-R, Lemma2.4.])Let r be a positive integer. Let K be a field and (V, ρ_V) be a finite dimensional linear representation of $\mathcal{F}_r$. Let $\lambda \in K^\times$. Then the subspaces*

$$\mathcal{K}_\lambda^{(r)}((V, \rho_V)) :=^t (\mathrm{Ker}(\rho_V(\sigma_1^{(r)}) - \mathrm{Id}_V), \dots, \mathrm{Ker}(\rho_V(\sigma_r^{(r)}) - \mathrm{Id}_V))$$

and

$$\mathcal{L}_\lambda^{(r)}((V, \rho_V)) := \bigcap_{i=1}^{r} \mathrm{Ker}(\mathrm{MC}_\lambda^{(r)}(\rho_V)(\sigma_i^{(r)}) - \mathrm{Id}_V)$$

of the underlying K-vector space of $\mathrm{C}_\lambda^{(r)}(V)$ are subrepresentations of $\mathcal{F}_r$.

Lemma 3.16. *([D-R, Lemma 2.7])Let r be a positive integer and $\lambda \in K^\times$. If $\lambda \neq 1$, then*

$$\mathcal{L}_\lambda^{(r)}((V, \rho_V)) = \{^t(u, \rho_V(\sigma_1^{(r)})u, \dots, \rho_V(\sigma_{r-1}^{(r)} \cdots \sigma_1^{(r)})u) | u \in \mathrm{Ker}(\lambda \rho_V(\sigma_1^{(r)} \cdots \sigma_r^{(r)}) - \mathrm{Id}_V)\}.$$

Then we define the middle convolution functor MC_λ for each $\lambda \in K^\times$.

Definition 3.17. *([D-R, Definition 2.5.])Let r be a positive integer. We define the middle convolution functor $\mathrm{MC}_\lambda^{(r)}$ for $\lambda \in K^\times$ from $\mathrm{Rep}_K(\mathcal{F}_r)$ to $\mathrm{Rep}_K(\mathcal{F}_r)$ as follows:*

$$\mathrm{MC}_\lambda^{(r)}((V, \rho_V)) := \mathrm{C}_\lambda^{(r)}((V, \rho_V)) / (\mathcal{K}^{(r)}((V, \rho_V)) + \mathcal{L}^{(r)}((V, \rho_V))).$$

Lemma 3.18. *([D-R, Lemma 2.7.])Let $\lambda \in K^\times \setminus 1$. Then*

$$\dim(\mathrm{MC}_\lambda((V, \rho_V))) = \sum_{i=1}^{r} \mathrm{rk}(\rho_V(\sigma_i) - \mathrm{Id}_V) - \dim\mathrm{Ker}(\lambda \rho_V(\sigma_1^{(r)}) \cdots \rho_V(\sigma_r^{(r)}) - \mathrm{Id}_V).$$

Remark 3.19. *Let* $(V, \rho_V), (V', \rho_{V'})$ *be objects of* $\mathrm{Rep}_K(\mathcal{F}_r)$ *such that* $V = V'$. *According to Lemma 3.18, if there exists elements* $g_i \in GL(V)$, $i = 1, \dots r$ *such that* $\rho_V(\sigma_i^r) = g_i \rho_{V'}(\sigma_i^r) g_i^{-1}$ *and* $\rho_V(\sigma_1^r \cdots \sigma_r^r) = \rho_{V'}(\sigma_1^r \cdots \sigma_r^r)$, *then the rank of* $\mathrm{MC}_\lambda(\rho_V)$ *is equal to the rank of* $\mathrm{MC}_\lambda(\rho_{V'})$ *for each* $\lambda \in K^\times$. *Moreover, if* $\rho_V(\sigma_1^r \cdots \sigma_r^r) = \rho_{V'}(\sigma_1^r \cdots \sigma_r^r) = \mathrm{Id}_V$, *then* $\mathcal{L}^{(r)}((V, \rho_V)) = \mathcal{L}^{(r)}((V, \rho_{V'})) = 0$ *(cf. Lemma 3.16) and the automorphism* ${}^t(g_1, \dots, g_r) : V^r \xrightarrow{\sim} V^r$ *induces an isomorphism*

$$\psi_{\rho_V, \rho_{V'}} : V^r / (\mathcal{K}^{(r)}(V, \rho_V)) \xrightarrow{\sim} V^r / \mathcal{K}^{(r)}((V, \rho_{V'}))$$

between the underlying K*-vector spaces of* $\mathrm{MC}_\lambda(\rho_V)$ *and* $\mathrm{MC}_\lambda(\rho_{V'})$ *for* $\lambda \in K^\times \setminus \{1\}$.

Lemma 3.20. *([D-R, Lemma 2.8.])The functor* $\mathrm{MC}_\lambda^{(r)}$ *commutes with direct sums for any positive integer* r *and* $\lambda \in K^\times$.

Lemma 3.21. *([D-R, Theorem 3.5])Let* r *be a positive integer. Let* (V, ρ_V) *be an object of* $\mathrm{Rep}_K(\mathcal{F}_r)$ *which satisfies one of the following conditions (a) and (b):*
(a) (V, ρ_V) *is irreducible and* $\mathrm{dim} V \geq 2$.
(b) The dimension of V *is equal to* 1 *and at least two of* $\rho_V(\sigma_i^{(r)})$ *are non trivial. Write* $(W, \rho_W) := \mathrm{MC}_\lambda((V, \rho_V))$. *Then*

$$\mathrm{rk}(\rho_V(\sigma_i^{(r)}) - \mathrm{Id}_V) = \mathrm{rk}(\rho_W(\sigma_i^{(r)}) - \mathrm{Id}_W)$$

for $i = 1, \dots r$ *and*

$$\mathrm{rk}(\lambda \rho_V(\sigma_1^{(r)}) \cdots \rho_V(\sigma_r^{(r)}) - \mathrm{Id}_V) = \mathrm{rk}(\rho_W(\sigma_1^{(r)}) \cdots \rho_W(\sigma_r^{(r)}) - \lambda\, \mathrm{Id}_W).$$

Definition 3.22. *([D-R])Let* $\Lambda := (\lambda_1, \dots, \lambda_r) \in (K^\times)^r$ *be an* r*-tuple of elements of* K. *The scalar multiplication functor* $\mathrm{M}_\Lambda^{(r)}$ *by* Λ *is defined as follows:*

$$\mathrm{M}_\Lambda(\rho)(\sigma_i^{(r)}) := \lambda_i \rho(\sigma_i^{(r)}) \ , \ 1 \leq i \leq r \ .$$

Lemma 3.23. *([D-R, Proposition 3.5,Theorem 3.6.])Let* r *be a positive integer. Let* $\mathcal{R}$ *be a full subcategory of* $\mathrm{Rep}_K(\mathcal{F}_r)$ *generated by objects which satisfy one of the conditions (a) and (b) in Lemma 3.21. Then the functor* $\mathrm{MC}_\lambda^{(r)}$ *(resp.* $\mathrm{M}_\Lambda^{(r)}$*) induces an equivalence of categories*

$$\mathrm{MC}_\lambda^{(r)}, \mathrm{M}_\Lambda^{(r)} : \mathcal{R} \xrightarrow{\quad \sim \quad} \mathcal{R}.$$

Quasi-inverses are $\mathrm{MC}_{\lambda^{-1}}^{(r)}$ *(resp.* $\mathrm{M}_{\Lambda^{-1}}^{(r)}$*). In particular, If* $V \in \mathcal{R}$ *and* $\lambda \in K^\times$, *then* V *is irreducible if and only if* $\mathrm{MC}_\lambda^{(r)}(V)$ *is irreducible.*

Lemma 3.24. *([D-R, Theorem 5.7.])Let r be a positive integer. Let $X \in \mathrm{Mat}_n(K)$ which satisfy ${}^tA_iXA_i = X$ for all $1 \leq i \leq r$. Let (V, ρ_V) be an object of $\mathrm{Rep}_K(\mathcal{F}_r)$ which is defined by $\rho_V(\sigma_i^{(r)}) := A_i$. Then we have*

$$ {}^t\,\mathrm{C}_{\lambda^{-1}}((V,\rho_V))(\sigma_i^{(r)})(Y_{k,l})_{k,l}\,\mathrm{MC}_\lambda^{(r)}((V,\rho_V))(\sigma_i^{(r)}) = (Y_{k,l})_{k,l}\ ,\ 1 \leq \forall i \leq r $$

where

$$ \mathrm{Y}_{k,l} := \begin{cases} X\lambda^{-1/2}(\lambda - A_k^{-1})(1-A_l) & (k = l) \\ X\lambda^{1/2}(A_k^{-1} - 1)(A_l - 1) & (k < l) \\ X\lambda^{-1/2}(A_k - 1)(A_l - 1) & (k > l). \end{cases} \tag{4} $$

for any integers k, l satisfying $1 \leq k, l \leq r$.

Corollary 3.25. *([D-R, Corollary 5.10.])Let (V, ρ_V) be an object of $\mathrm{Rep}_K(\mathcal{F}_r)$. If $\mathrm{Im}(\rho_V)$ is a subgroup of a symplectic group of rank n (resp. orthogonal group of rank n), then $\mathrm{Im}(\mathrm{MC}_{-1}(\rho_V))$ is a subgroup of an orthogonal group of rank m(resp. symplectic group of rank m) where*

$$ m = \sum_{i=1}^{r} \mathrm{dimKer}(\rho_V(\sigma_i^{(r)}) - \mathrm{Id}_V) - \mathrm{dimKer}(-\rho_V(\sigma_1^{(r)}) \cdots \rho_V(\sigma_r^{(r)}) - \mathrm{Id}_V). $$

Definition 3.26. *Let r be a positive integer and $V = (V, \rho_V)$ be an object of $\mathrm{Rep}_K(\mathcal{F}_r)$. Then we define a representation $\mathcal{S}(V) = (V, S(\rho_V))$ of $\mathcal{F}_{r-1}$ by*

$$ \mathcal{S}(\rho_V)(\sigma_i^{(r-1)}) := \begin{cases} \rho_V(\sigma_i^{(r)}) & (i \neq r-1) \\ \rho_V(\sigma_{r-1}^{(r)}\sigma_r^{(r)}) & (i = r-1) \end{cases} $$

Lemma 3.27. *([D-R, Lemma 5.6.])Let r be a positive integer. Let (V, ρ_V) be a representation of $\mathcal{F}_r$ over a field K and $\lambda \in K^\times$. Then there exists a surjective group homomorphism*

$$ \mathrm{Im}(\mathcal{S}(MC_\lambda^{(r)}(\rho_V))) \twoheadrightarrow \mathrm{Im}(\mathrm{MC}_\lambda^{(r-1)}(\rho_{\mathcal{S}(V)}))\ . $$

3.4 Linearly Rigidity

In this section, we define linearly rigid r-tuples of $GL(V)$ and give a criterion of the linearly rigidity.

Definition 3.28. *Let K be a field and r be a positive integer.*
(1) Let V be a K-vector space and $(g_1, \ldots, g_r)$ be an r-tuple of elements of $GL(V)$. We say that $(g_1, \ldots, g_r)$ is linearly rigid if for any $g'_i = h_ig_ih_i^{-1}$, $h_i \in GL(V)$, which satisfy the condition $(g'_1 \cdots g'_r) = h_\infty(g_1 \cdots g_r)h_\infty^{-1}$ for some $h_\infty \in GL(V)$, then there exists an element g which does not depend on i of $GL(V)$ such that $g'_i = gg_ig^{-1}$, $g'_1 \cdots g'_r = gg_1 \cdots g_rg^{-1}$.
(2) Let $V = (V, \rho_V)$ be a linear representation of $\mathcal{F}_r$ over K. We say that V is linearly rigid if $(\rho_V(\sigma_1^{(r)}), \ldots, \rho_V(\sigma_r^{(r)}))$ is linearly rigid.

Remark 3.29. *A linearly rigid r-tuple $(g_1, \dots, g_r)$ is not rigid tuple of the group $\langle g_1, \dots, g_r \rangle$ in general. For example, if the normalizer $N_{GL(V)}(\langle g_1, \dots, g_r \rangle)$ of $\langle g_1, \dots, g_r \rangle$ in $GL(V)$ is not equal to $K^\times \langle g_1, \dots, g_r \rangle$, then $\mathcal{E}^{\mathrm{in}}((g_1, \dots, g_r))$ is not singleton.*

Proposition 3.30. *Let K be a field and r be a positive integer. Let V be a K-vector space and $(g_1, \dots, g_r)$ be a linearly rigid r-tuple of elements of $GL(V)$ which satisfies the condition $g_1 \cdots g_r = 1$.*
(1) Then there exists a subgroup J of $N_{GL(V)}(\langle g_1, \dots, g_r \rangle)$ such that J acts on $\mathcal{E}^{\mathrm{in}}(\mathcal{C}((g_1, \dots, g_r)))$ transitively. Here, $\mathcal{C}((g_1, \dots, g_r)) = (C(g_1), \dots, C(g_r))$ is the r-tuple of conjugacy classes of $\langle g_1, \dots, g_r \rangle$ such that $C(g_i)$ contains g_i and $N_{GL(V)}(\langle g_1, \dots, g_r \rangle)$ is the normalizer of $\langle g_1, \dots, g_r \rangle$ in $GL(V)$.
(2) Moreover, the group J satisfies the condition (b) of Theorem 3.2 (resp. the condition for H of Theorem 3.4), the group $\langle g_1, \dots, g_r \rangle / Z(\langle g_1, \dots, g_r \rangle)$ is regular over $\mathbb{Q}_{\mathcal{C}}(\mu_m)$ (resp. $\mathbb{Q}_{\mathcal{C}}$) where m is defined same as Theorem 3.3.

Proof. The assertion of (1) is almost the definition of the linearly rigidity.

The assertion of (2) follows Theorem 3.2 (resp. Theorem 3.4) with $\mathcal{C} = \mathcal{C}((g_1, \dots, g_r))$ and $J = H$. □

Lemma 3.31. *([D-R, Lemma 4.7.])Let r be a positive integer and K be a field. Let $(g_1, \dots, g_r)$ be an r-tuple of elements of $GL_n(K)$ which satisfies the condition $g_1 \dots g_r = 1$. Then $(g_1, \dots, g_r)$ is linearly rigid if and only if*

$$\sum_{i=1}^{r} \dim_K(C_{\mathrm{Mat}_n(K)}(g_i)) - (r-2)n^2 = 2 \tag{5}$$

where $C_{\mathrm{Mat}_n(K)}(g_i)$ is the centralizer of g_i in $\mathrm{Mat}_n(K)$.

Definition 3.32. *([D-R, Definition 4.3.])Let r be a positive integer. and K be a field. Let $(g_1, \dots, g_r)$ be an r-tuple of elements of $GL_n(K)$ which satisfies the condition $g_1 \dots g_r = 1$. We call left hand side of equation (5) index of rigidity of $(g_1, \dots, g_r)$.*

Lemma 3.33. *([D-R, Corollary 4.4.])Let V be a linear representation of $\mathcal{F}_r$ over K. If V is linearly rigid and satisfies the condition (a) or (b) of Lemma 3.21, then $\mathrm{MC}_\lambda^{(r)}(V)$ is also linearly rigid for all $\lambda \in K^\times$.*

3.5 Realization of Some orthogonal Groups (1)

In this section, we give an application of Main Theorem A.

Definition 3.34. *Let K be a field and V be a K-vector space. Let r be a positive integer and $\mathbb{T} = (T_1, \dots, T_r)$ be an r-tuple of elements of $GL(V)$.*
(1) We define the representation $(V, \rho_{\mathbb{T}})$ of $\mathcal{F}_r$ on V which corresponds to $\mathbb{T}$ as follows: $(V, \rho_{\mathbb{T}})$ is defined by

$$\rho_{\mathbb{T}}(\sigma_i^{(r)}) := T_i \ , \ i = 1, \dots, r.$$

Conversely, we define an r-tuple $\mathbb{T}_V$ of elements of $GL(V)$ which corresponds to a representation (V, ρ_V) of $\mathcal{F}_r$ by $\mathbb{T}_V := (\rho_V(\sigma_1^{(r)}), \ldots, \rho_V(\sigma_r^{(r)}))$.
(2) Let C be a subcategory of $\mathrm{Rep}_K(\mathcal{F}_r)$ and $F : C \to \mathrm{Rep}_K(\mathcal{F}_r)$ be a functor. We define an r-tuple $F(\mathbb{T})$ of elements of $GL(W)$ by the above correspondence. Here W is the underlying K-vector space of $F((V, \rho_{\mathbb{T}}))$
(3) We denote by $\langle \mathbb{T} \rangle$ the subgroup of $GL(V)$ which is generated by $\{T_i\}_{i=1,\ldots,r}$.

Proposition 3.35. *Let p be an odd prime and n be an even natural number. If $p \equiv 7 \pmod{12}$, $4|n$ and $n \geq 12$ hold, then $PSO_n^+(\mathbb{F}_p)$ is regular over $\mathbb{Q}$.*

Proof. Let $\zeta_3 \in \mathbb{F}_p^\times$ be a primitive cubic root of unity. We take a $(2m+3)$-tuple of elements $\mathbb{T}$ of $SL_2(\mathbb{F}_p)$ as follows:

$$\mathbb{T}_0 := (-E_2, \ldots, -E_2, g_1, g_2, g_3) \tag{6}$$

where

$$g_1 := \begin{pmatrix} \zeta_3 & 0 \\ 0 & \zeta_3^{-1} \end{pmatrix} \tag{7}$$

and

$$g_2 := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \tag{8}$$

and

$$g_3 := -g_2^{-1} g_1^{-1} = \begin{pmatrix} 0 & -\zeta_3^{-1} \\ \zeta_3 & 0 \end{pmatrix}. \tag{9}$$

Here E_2 is the identity matrix of degree 2. We assume that $m > 1$. The index of rigidity (cf. Definition 3.32) of $(\mathbb{T}_0, -E_2)$ is equal to 2, so $\mathbb{T}_0$ is linearly rigid (cf. Lemma 3.31). We define the $(2m+3)$-tuple $(U_1, U_2, \ldots, U_{2m}, G_1, G_2, G_3)$ of elements of $GL(W)$ as follows:

$$(U_1, \ldots, U_{2m}, G_1, G_2, G_3) := \mathrm{MC}_{-1}^{(2m+3)}(\mathbb{T}).$$

Here W is the underlying $\mathbb{F}_p$-vector space of $\mathrm{MC}_{-1}^{(2m+3)}(\rho_{\mathbb{T}})$ (cf. Definition 3.34). By the definition of convolution functors and Lemma 3.21, we conclude that U_i are unipotent biperspectivities and G_1 is a semi-simple biperspectivity with eigenvalues $-\zeta_3, -\zeta_3^{-1}$. According to Lemma 3.21, we have $U_1 U_2 \cdots U_{2m} G_1 G_2 G_3 = -\mathrm{Id}_W$. We denote $(-U_1, U_2, \ldots, U_{2m}, G_1, G_2, G_3)$ by $\tilde{\mathbb{T}}$ for short. According to Lemma 3.18, the dimension of W over $\mathbb{F}_p$ is equal to $2(2m+3) - 2 = 2(2m+2)$.

First, we prove the proposition under the assumption that the following claims are true.

Claim 1. *The group $\langle \tilde{\mathbb{T}} \rangle$ is isomorphic to $SO^+_{2(2m+2)}(\mathbb{F}_p)$.*

Claim 2. *Let $C(U_i)$, $i = 1, \ldots 2m$ (resp. $C(G_j)$, $j = 1, 2, 3$) be the conjugacy class of $\langle \tilde{\mathbb{T}} \rangle$ which contains U_i(resp. G_j). Then the $(2m+3)$-tuple of conjugacy classes $\mathcal{C}(\tilde{\mathbb{T}}) := (-C(U_1), \ldots C(U_{2m}), C(G_1), C(G_2), C(G_3))$ of $\langle \tilde{\mathbb{T}} \rangle$ is rational.*

Let $\{w_1, \ldots, w_{2m+2}, w'_1, \ldots, w'_{2m+2}\}$ be a standard basis of $(W, (\ ,\ ))$ in the sense of [K-L, Proposition 1.2, 5.3.(1)]. According to [K-L, Proposition 1.2, 7.3 (3)], the outer automorphism group of $SO(W, (\ ,\ ))$ is generated by the images of δ , γ where $\gamma \in GO(W, (\ ,\ ))$ is a reflection and

$$\delta : w_i \mapsto -w_i\ ,\ w'_i \mapsto w'_i\ ,\ i = 1, \ldots, 2m+2.$$

Put $\gamma' := \delta\gamma\delta^{-1}$. Note that the action of $\langle\, \gamma, \gamma', \delta \,\rangle$ on $\mathcal{E}^{\mathrm{in}}_{2m+3}(SO(W, (\ ,\ )))$ factors through the canonical surjection

$$(\mathbb{Z}/2\,\mathbb{Z})^2 \rtimes S_2 \cong \langle\, \gamma, \gamma', \delta \,\rangle \twoheadrightarrow \langle\, \gamma, \gamma', \delta \,\rangle \,/\, \langle\, \gamma\gamma' \,\rangle \cong (\mathbb{Z}/2\,\mathbb{Z})^2$$

because $\gamma\gamma' \in SO(W, (\ ,\ ))$.

Since $\tilde{\mathbb{T}}$ is linearly rigid(cf. Proposition 3.33), there exists a subgroup J' of $\mathrm{Aut}_{\mathcal{C}(\tilde{\mathbb{T}})}(SO(W, (\ ,\ )))$ such that the action of J' on the set $\mathcal{E}^{\mathrm{in}}(\mathcal{C}(\tilde{\mathbb{T}}))$ is transitive (cf. Proposition 3.30 (1)). Then we have the regularity of $PSO^{+}_{2(2m+2)}(\mathbb{F}_p)$ over $\mathbb{Q}$ by applying Proposition 3.30 (2) with $r = 2m+3$, $J = J' \cap \langle\, \gamma, \gamma', \delta \,\rangle$ and $(g_1, \ldots, g_r) = (-U_1, \ldots, U_{2m}, G_1, G_2, G_3)$.

Let us prove Claim 1. First, we prove that $\langle\, \tilde{\mathbb{T}} \,\rangle$ is a primitive subgroup of $GL(W)$. Note that the group $\langle\, \tilde{\mathbb{T}} \,\rangle$ is a absolutely irreducible subgroup of $GL(W)$ (cf. Lemma 3.23). Assume that $\langle\, \tilde{\mathbb{T}} \,\rangle$ is not a primitive subgroup of $GL(W)$. By assumption, there exists a decomposition $\oplus_{i=1}^{l} V_i = W$ for some integer $l > 1$ such that $\langle\, \tilde{\mathbb{T}} \,\rangle$ acts on $\{V_i\}_{i=1}^{l}$ by permutation. By applying Lemma 3.8, we have

$$\mathrm{dim} V_1 \geq 2(2m+2) - \frac{1}{2}(2(2m+3)) + \frac{1}{2}(a+b) = 2m+1+\frac{1}{2}(a+b)$$

where a and b are non-negative integer which are defined in Lemma 3.8. Since $m > 1$, we have $2m+1 > 3$. Since the ranks of $(G_i - \mathrm{Id}_W)$ for $i = 1, 2, 3$ are 2 (cf. Lemma 3.21), then we have $a + b \geq 6$. Thus $\mathrm{dim} V_1 > \frac{1}{2}\mathrm{dim} V$, and $\langle\, \tilde{\mathbb{T}} \,\rangle$ stabilize V_1. But $\langle\, \tilde{\mathbb{T}} \,\rangle$ is an irreducible subgroup of W (cf. Lemma 3.23), which is contradiction.

We determine the group which is generated by $\tilde{\mathbb{T}}$. According to Corollary 3.25, there exists a symmetric form $(\ ,\ )$ on W and $\langle\, \tilde{\mathbb{T}} \,\rangle$ is a primitive irreducible subgroup of $SO(W, (\ ,\ ))$. According to Lemma 3.27, there exists a surjective group homomorphism

$$\langle\, \mathcal{S}(\tilde{\mathbb{T}}) \,\rangle \twoheadrightarrow \langle\, MC_{-1}^{(2m+2)}(\mathcal{S}(\mathbb{T}_0)) \,\rangle\, .$$

Let $V := \mathbb{F}_p^2 = V_1 \oplus V_2$ be the irreducible decomposition of V as a representation of $\langle\, \mathcal{S}(\mathbb{T}) \,\rangle$. Then we have a decomposition $MC_{-1}^{(2m+2)}(V) = MC_{-1}^{(2m+2)}(V_1) \oplus MC_{-1}^{(2m+2)}(V_2)$ as a representation of $\langle\, MC_{-1}^{(2m+2)}(\mathcal{S}(\mathbb{T}_0)) \,\rangle$ (cf. Lemma 3.20). By the definition of $\mathbb{T}$, $MC_{-1}^{(2m+2)}(V_1)$ is isomorphic to $MC_{-1}^{(2m+2)}(\rho_{\mathbb{T}'})$ as $\mathcal{F}_{2(2m+2)}$-modules. Here $\mathbb{T}'$ is a $(2m+2)$-tuple of elements of $GL_1(\mathbb{F}_p)$ which is defined by

$$\mathbb{T}' := (-1, \ldots, -1, \zeta_3, -\zeta_3^{-1}).$$

The group $\langle\, MC_{-1}^{(2m+2)}(\mathbb{T}')\,\rangle$ has a subgroup which is isomprphic to $SL_{2m+1}(\mathbb{F}_p)$ because $\langle\, MC_{-1}^{(2m+2)}(\mathbb{T}')\,\rangle$ is isomorphic to an irreducible primitive subgroup of $GL_{2m+1}(\mathbb{F}_p)$ and contains a homology of order 3 (cf. Lemma 3.6). By the classification of the maximal subgroup of orthogonal groups over finite fields ([K-L, Table 3.5.E, 3.5.F]), we conclude that $\langle\,\tilde{\mathbb{T}}\,\rangle$ contains the maximal subgroup of $\Omega(W,(\ ,\ ))\cong\Omega^{+}_{2(2m+2)}(\mathbb{F}_p)$ of type $\mathcal{C}_2$ in the sense of [K-L, Section 4.2.] or contains $\Omega(W,(\ ,\ ))\cong\Omega^{+}_{2(2m+2)}(\mathbb{F}_p)$. But the maximal subgroups of $\Omega(W,(\ ,\ ))$ of type $\mathcal{C}_2$ are imprimitive subgroup of $GL(W)$. Thus we conclude that the group $\langle\,\tilde{\mathbb{T}}\,\rangle$ contains $\Omega(W,\ (\ ,\ ))$. The value of the spinor norm of G_1 is not 1 because -1 is not square in $\mathbb{F}_p$. So we conclude that $\langle\,\tilde{\mathbb{T}}\,\rangle = SO(W,(\ ,\ ))\cong SO^{+}_{2(2m+2)}(\mathbb{F}_p)$.

Let us prove Claim 2. Since $C(U_i)$ and $C(G_1)$ are rational conjugacy classes (Corollary 3.11, Lemma 3.12), it is sufficient to prove that the 2-tuple of conjugacy classes $(C(G_2),C(G_3))$ is rational. It is sufficient to prove that $C(G_2)^3=C(G_3)$ because the orders of G_2 and G_3 are 4.

Put

$$W_2' := \begin{pmatrix} 0\\ \vdots\\ *\\ *\\ 0\\ 0 \end{pmatrix}\ ,\ W_3' := \begin{pmatrix} 0\\ \vdots\\ 0\\ 0\\ *\\ * \end{pmatrix} \tag{10}$$

the subspace of the underlying $\mathbb{F}_p$-subspace of $\mathrm{C}_{-1}^{(2m+3)}(\rho_{\mathbb{T}})$. Here we identify $(\mathbb{F}_p^2)^r$ with $\mathbb{F}_p^{2r}$ by the isomorphism from $(\mathbb{F}_p^2)^r$ to $\mathbb{F}_p^{2r}$ as follows:

$$\begin{pmatrix} \begin{pmatrix} a_1\\ a_2 \end{pmatrix}\\ \begin{pmatrix} a_3\\ a_4 \end{pmatrix}\\ \vdots\\ \begin{pmatrix} a_{2r-1}\\ a_{2r} \end{pmatrix} \end{pmatrix} \longmapsto \begin{pmatrix} a_1\\ a_2\\ a_3\\ a_4\\ \vdots\\ a_{2r-1}\\ a_{2r} \end{pmatrix} \quad a_1,a_2,\ldots,a_{2r}\in\mathbb{F}_p. \tag{11}$$

Let W_i be the image of W_i' in $\mathrm{MC}_{-1}^{(2m+3)}(\mathbb{T})$. According to Lemma 3.16, $\mathbb{F}_p$-vector spaces W_i and W_i' are isomorphic for $i=2,3$, so we identify W_i with W_i'. Let $\{e_j\}_{j=1,2}$ (resp. $\{e_j'\}_{j=1,2}$ be a basis of W_2 (resp W_3) which is defined as follows:

$$e_1 := \begin{pmatrix} 0\\ \vdots\\ 1\\ 0\\ 0\\ 0 \end{pmatrix}\ ,\ e_2 := \begin{pmatrix} 0\\ \vdots\\ 0\\ 1\\ 0\\ 0 \end{pmatrix}\ ,\ e_1' := \begin{pmatrix} 0\\ \vdots\\ 0\\ 0\\ 1\\ 0 \end{pmatrix}\ ,\ e_2' := \begin{pmatrix} 0\\ \vdots\\ 0\\ 0\\ 0\\ 1 \end{pmatrix} \tag{12}$$

According to Lemma 3.24, the matrix representation X_2 (resp. X_3) of the restrictions of the symmetric form $(\ ,\ )$ to W_2 (resp. W_3) with respect to the base $\{e_j\}_{j=1,2}$ (resp.$\{e'_j\}_{j=1,2}$) is written as follows:

$$X_2 = (-1)^{1/2} g_2(-1-g_2^{-1})(1-g_2) = -(-1)^{1/2} g_2(1-g_2)^2 = -2(-1)^{1/2} E_2$$

$$(\text{resp. } X_3 = (-1)^{1/2} g_2(-1-g_3^{-1})(1-g_3) = -2(-1)^{1/2} g_1^{-1}.\ )$$

Since these forms are non-degenerate, we have the orthogonal decompositions $V = W_i \perp W_i^{\perp}$ for $i = 2,3$. Since G_i preserve W_i and $W_i^{\perp}$, there exist automorphisms u_i of $W_i^{\perp}$ for $i = 2,3$ such that $G_i = G_i|_{W_i} \oplus u_i$. The order of u_i are divided by 4 because the order of G_i are 4 for $i = 2,3$. But u_i are unipotent and p is not even, so we have $u_i = \mathrm{Id}_{W_i^{\perp}}$ for $i = 2,3$.

Define an isometry

$$g : W_2 \xrightarrow{\sim} W_3\ ,\ e_1 \mapsto \zeta_3^{-1} e'_1\ ,\ e_2 \mapsto \zeta_3 e'_2\ .$$

By applying Witt's Lemma for $(W, (\ ,\ ), g)$ ([K-L, Proposition 1.2, 1.6.]), the isometry g can be extended to an element of $SO(W, (\ ,\ ))$. Let $\tilde{g}$ be an element of $SO(W, (\ ,\ ))$ such that $\tilde{g}|_{W_2} = g$. By the definition of G_i and $\tilde{g}$, we have $\tilde{g} G_2 \tilde{g}^{-1} = G_3^3$. Thus $(C(G_2), C(G_3))$ is rational.

This completes the proof of the proposition. $\square$

4 Second Main Theorem and Applications

In this section, we prove the regularity of the groups $\langle\, \mathrm{MC}_\lambda^{(r)}(\mathbb{T})\,\rangle / Z(\langle\, \mathrm{MC}_\lambda^{(r)}(\mathbb{T})\,\rangle)$ over $\mathbb{Q}$ for some $\mathbb{T}$ which is not linearly rigid. The main tool is the action of the braid group on $\mathrm{Rep}_K(\mathcal{F}_r)$.

4.1 Braiding Actions and Middle Convolution Functors

First, we define the braid groups A_r on r-strands and define the action of A_r on $\mathrm{Rep}_K(\mathcal{F}_r)$.

Definition 4.1. *([D-R, Section 5]) Let r be a positive integer.*
(1)The braid group A_r on r-strands is defined as follows:
$A_r := \left\langle P_i, 1 \le i \le r-1 \,\middle|\, P_i P_{i+1} P_i = P_{i+1} P_i P_{i+1}\ ,\ [P_i, P_j] = 1 |i-j| \ge 2 \right\rangle$
(2) The pure braid group $A^{(r)}$ on r-strands is the kernel of the group homomorphism

$$A_r \to S_r\ ,\ P_i \mapsto (i, i+1)\ ,\ i = 1, \ldots, r-1$$

where S_r is the symmetric group of degree r.

Definition 4.2. *Let r be a positive integer and A_r be the braid group on r-strands.*

(1) We define the group homomorphism $\nu : A_r \to \mathrm{Aut}(\mathcal{F}_r)$ as follows:

$$\nu(P_i)(\sigma_j^{(r)}) := \begin{cases} \sigma_j^{(r)} & (|j-i|>1, \text{ or } j<i) \\ \sigma_i^{(r)}\sigma_{i+1}^{(r)}{\sigma_i^{(r)}}^{-1} & (j=i) \\ \sigma_i^{(r)} & (j=i+1)\ . \end{cases}$$

(2) The functor $F_P : \mathrm{Rep}_K(\mathcal{F}_r) \to \mathrm{Rep}_K(\mathcal{F}_r)$ is defined for each $P \in A_r$ as follows:

$$F_P(\rho) := \rho \circ \nu(P).$$

(3) Let $\mathbb{T} = (T_1, \dots, T_r)$ be an r-tuple of elements of $GL(V)$ where V is a K-vector space. We define the action of A_r on $\mathcal{E}_r^{\mathrm{in}}(\langle \mathbb{T} \rangle)$ as follows:

$$P[\mathbb{X}] := [F_P(\rho_{\mathbb{X}})(\sigma_1^{(r)}), \dots, F_P(\rho_{\mathbb{X}})(\sigma_r^{(r)})]\ ,\ P \in A_r, [\mathbb{X}] \in \mathcal{E}_r^{\mathrm{in}}(\langle \mathbb{T} \rangle)$$

where $\rho_{\mathbb{X}}$ is an object of $\mathrm{Rep}_K(\mathcal{F}_r)$ which is defined by $\rho_{\mathbb{X}}(\sigma_i^{(r)}) := X_i$ (cf. Definition 3.34).

Remark 4.3. *The braid group A_r on r-strands is isomorphic to the topological fundamental group of the topological space $\mathcal{U}_r'$ where*

$$\mathcal{U}_r' := \{\{x_1, \dots, x_r\} |\ x_i \in \mathbb{C},\ x_i \neq x_j \text{ if } i \neq j\}.$$

The topological space $\mathcal{U}_r'$ is an open set of $\mathcal{U}_r(\mathbb{C})$ and the canonical inclusion from $\mathcal{U}_r'$ to $\mathcal{U}_r(\mathbb{C})$ induces the canonical projection $A_r \twoheadrightarrow B_r$, $P_i \mapsto Q_i$, $i = 1, \dots, r-1$.

The following property is an important property of the functor F_P.

Proposition 4.4. *([D-R, Theorem 5.1])Let r be a positive integer. Then, there exist isomorphisms of functors*

$$C_\lambda^{(r)} \circ F_P \cong F_P \circ C_\lambda^{(r)}\ ,\ MC_\lambda^{(r)} \circ F_P \cong F_P \circ MC_\lambda^{(r)}\ ,\ M_\Lambda^{(r)} \circ F_P \cong F_P \circ M_\Lambda^{(r)}$$

for all $\lambda \in K, \Lambda \in (K^\times)^r, P \in A_r$.

We introduce some tuple of elements of $GL_n(\mathbb{F}_q)$ which is used in Main Theorem B.

Lemma 4.5. *([D-R, Lemma.7.2.])Let r be a positive integer. Let $H \subset GL_n(\mathbb{F}_q)$ be the semi-direct product of the group D of diagonal elements with ρ where ρ is the matrix which represents a cyclic permutation of order n. Let $\mathbb{T} := (T_1, \dots, T_r)$ be an r-tuple of elements of H consisting of two elements T_1, T_2 whose action on D by conjugation are cyclic permutations of order n, k homologies $T_3, \dots, T_{k+2} \in D$, $k \geq 1$, and $r-(k+2)$ central elements such that $T_1 \cdots T_r = 1$. Then, the pure braid group $A^{(r)}$ acts transitively as abelian group isomorphic to $(\mathbb{Z}/n\mathbb{Z})^{k-1}$ on $\mathcal{E}^{\mathrm{in}}(\mathcal{C})$. Here $\mathcal{C} = (C_1, \dots C_r)$ is the r-tuple of conjugacy classes of $\langle \mathbb{T} \rangle$ such that C_i is the conjugacy class of T_i for each i.*

Lemma 4.6. *Let K be a field and n be a positive integer. Let $\rho \in GL_n(K)$ be an invertible matrix which satisfies the following condition:*

$$\rho^{-1}\mathrm{diag}(y_1, y_2, \dots y_n)\rho = \mathrm{diag}(y_n, y_1, \dots, y_{n-1}) \ , \ \forall y_i \in K^{\times} \ .$$

Then, the following equation holds:

$$\mathrm{diag}(1, x_2, x_2x_3, \dots, \prod_{i=2}^{n} x_i)\rho\mathrm{diag}(x_1, x_2, \dots, x_n)\mathrm{diag}(1, x_2, x_2x_3, \dots, \prod_{i=2}^{n} x_i)^{-1} = \rho\mathrm{diag}(\prod_{i=1}^{n} x_i, 1, \dots, 1) \ , \ \forall x_i \in K^{\times}.$$

Here $\mathrm{diag}(x_1, \dots x_n)$ *is the diagonal matrix whose (i,i) component is equal to x_i.*

We omit to prove Lemma 4.6 because this follows from an elementary calculation.

We recall the definition of Nielsen classes for the later lemma.

Definition 4.7. *(Nielsen classes [Fr-Vö, Section 1.1.]) Let r be a positive integer. Let G be a finite group and $\mathcal{C} = (C_1, \dots, C_r)$ be an r-tuple of conjugacy classes of G. The Nielsen class $\mathcal{N}^{\mathrm{in}}(\mathcal{C})$ of $\mathcal{C}$ is defined as follows:*

$$\mathcal{N}^{\mathrm{in}}(\mathcal{C}) := \{[g_1, \dots, g_r] \in \mathcal{E}_r^{\mathrm{in}}(G) \mid g_{\sigma(i)} \in C_i \ 1 \le i \le r \ , \ \exists \sigma \in S_r\}$$

where S_r is the symmetric group of degree r.

Next, we define a subset of $\mathcal{E}_r^{\mathrm{in}}(\langle \mathrm{MC}_\lambda(\mathbb{T}) \rangle)$ which plays an important role in the proof of Main Theorem B .

Definition 4.8. *Let r be a positive integer and $\mathbb{T} = (T_1, \dots, T_r)$ be an r-tuple of elements of $GL_n(\mathbb{F}_q)$ such that $\rho_{\mathbb{T}}$ satisfies the condition (a) or (b) of Lemma 3.21. Let F be a functor which is an iterated composition of middle convolutions and scalar multiplications. Let $\tilde{\mathbb{T}} = (\tilde{T}_1, \dots, \tilde{T}_r)$ be an r-tuple of elements of $GL(V)$ which is defined by $\tilde{\mathbb{T}} := F(\mathbb{T})$. Here, V is the underlying $\mathbb{F}_q$-vector space of $\rho_{\tilde{\mathbb{T}}}$. Define the subset $\mathcal{N}_{\mathbb{T}}^{\mathrm{in}}(\tilde{\mathbb{T}}, F)$ of $\mathcal{E}_r^{\mathrm{in}}(\langle \tilde{\mathbb{T}} \rangle)$ as follows:*

$$\mathcal{N}_{\mathbb{T}}^{\mathrm{in}}(\tilde{\mathbb{T}}, F) := \{[\mathbb{X}] \in \mathcal{N}^{\mathrm{in}}(\mathcal{C}) \mid h\langle (F|_{\mathcal{R}})^{-1}(\mathbb{X})\rangle h^{-1} = \langle \mathbb{T} \rangle \ , \exists h \in GL_n(\mathbb{F}_q)\}$$

Here, $\mathcal{C} = (C_1, \dots, C_r)$ is the r-tuple of conjugacy classes of $\langle \tilde{\mathbb{T}} \rangle$ such that C_i contains $\tilde{T}_i$ and fix an isomorphism of functors $(F|_{\mathcal{R}})^{-1} \circ F|_{\mathcal{R}} \cong \mathrm{Id}$ and we regard the underlying $\mathbb{F}_q$-vector space of $(F|_{\mathcal{R}})^{-1}(\rho_{\mathbb{X}})$ as $\mathbb{F}_q^n$ by using the above isomorphism and the isomorphism $\psi_{\rho_{\mathbb{X}}, \rho_{\tilde{\mathbb{T}}}}$ (cf. Remark 3.19, Lemma 3.23).

Lemma 4.9. *Let r be a positive integer and λ be an element of $K^{\times}$ and Λ be an element of $(K^{\times})^r$. Let $\mathbb{T} = (T_1, \dots, T_r)$ be an r-tuple of elements of $GL_n(\mathbb{F}_q)$ as Lemma 4.5. Define an r-tuple $\tilde{\mathbb{T}} = (\tilde{T}_1, \dots, \tilde{T}_r)$ of elements of $GL(W)$ by $\tilde{\mathbb{T}} := \mathrm{MC}_\lambda^{(r)}(\mathbb{T})$ (resp. $\tilde{\mathbb{T}} := \mathrm{M}_\Lambda^{(r)}(\mathbb{T})$) where W is the underlying*

$\mathbb{F}_q$-vector space. Let $\mathcal{C} = (C_1, \dots C_r)$ be the r-tuple of the conjugacy class of $\langle \tilde{\mathbb{T}} \rangle$ such that C_i contains T_i. Then $N_{GL(V)}(\langle \tilde{\mathbb{T}} \rangle) \times A_r$ acts on $\mathcal{N}^{\mathrm{in}}_{\mathbb{T}}(\tilde{\mathbb{T}}, \mathrm{MC}^{(r)}_{\lambda})$ (resp. $\mathcal{N}^{\mathrm{in}}_{\mathbb{T}}(\tilde{\mathbb{T}}, \mathrm{M}^{(r)}_{\Lambda})$) transitively. Here V is the underlying $\mathbb{F}_q$-vector space of $\rho_{\tilde{\mathbb{T}}}$.

Proof. By definition of $\mathcal{N}^{\mathrm{in}}_{\mathbb{T}}(\tilde{\mathbb{T}}, \mathrm{MC}^{(r)}_{\lambda})$, the group $N_{GL(V)}(\langle \tilde{\mathbb{T}} \rangle) \times A_r$ acts on $\mathcal{N}^{\mathrm{in}}_{\mathbb{T}}(\tilde{\mathbb{T}}, \mathrm{MC}^{(r)}_{\lambda})$. We prove that this action is transitive.

Take an element $[\mathbb{X}] = [(X_1, \dots X_r)]$ of $\mathcal{N}^{\mathrm{in}}_{\mathbb{T}}(\tilde{\mathbb{T}}, \mathrm{MC}^{(r)}_{\lambda}) \cap \mathcal{E}^{\mathrm{in}}_r(\langle \tilde{\mathbb{T}} \rangle)$ and put $(S_1, \dots, S_r) := MC^{(r)}_{\lambda^{-1}}(\mathbb{X})$. By the definition of the set $\mathcal{N}^{\mathrm{in}}_{\mathbb{T}}(\tilde{\mathbb{T}}, \mathrm{MC}^{(r)}_{\lambda})$, there exists an element h of $GL_n(\mathbb{F}_q)$ such that $h \langle S_1, \dots, S_r \rangle h^{-1} = \langle \mathbb{T} \rangle$. According to Lemma 3.21, S_i are homology whose eigenvalues are same as T_i for $3 \leq i \leq k+2$. In particular hS_ih^{-1} and T_i are conjugate in $\langle \mathbb{T} \rangle$ for $3 \leq i \leq k+2$. By using the explicit description of middle convolution functors, we conclude that the eigenvalues of the element S_i are same values for $i = k+3, \dots, r$. Since hS_ih^{-1} are diagonalizable for each $i = 1, \dots, r$, we have $S_i = T_i$ for each $i = k+3, \dots, r$. The conjugate action of hS_1h^{-1}(resp. hS_2h^{-1}) on the normal subgroup $D \cap \langle \mathbb{T} \rangle$ of $\langle \mathbb{T} \rangle$ is a cyclic permutation of order n because the set $\{hS_1h^{-1}, \dots hS_rh^{-1}\}$ generates $\langle \mathbb{T} \rangle$. By using the explicit description of middle convolution functors, the determinant of S_1 (resp. S_2) is same as the determinant of T_1 (resp. T_2). According to Lemma 4.6 any two cyclic permutation matrices in $\langle \mathbb{T} \rangle$ of order n whose determinants are same value are conjugate in $\langle \mathbb{T} \rangle$. Thus the element $[hS_1h^{-1}, \dots, hS_rh^{-1}] \in \mathcal{E}^{\mathrm{in}}_r(\langle \mathbb{T} \rangle)$ is an element of $\mathcal{E}^{\mathrm{in}}(\mathcal{C}')$. Here $\mathcal{C}' = (C(T_1), \dots C(T_r))$ is the r-tuple of conjugacy classes of $\langle \mathbb{T} \rangle$ such that $C(T_i)$ contains T_i.

Take an element $[\mathbb{Y}]$ of $\mathcal{N}^{\mathrm{in}}_{\mathbb{T}}(\tilde{\mathbb{T}}, \mathrm{MC}^{(r)}_{\lambda})$. By the definition of the action of braid groups, there exists an element P_1 of A_r such that $P_1[\mathbb{Y}]$ is an element of $\mathcal{N}^{\mathrm{in}}_{\mathbb{T}}(\tilde{\mathbb{T}}, \mathrm{MC}^{(r)}_{\lambda}) \cap \mathcal{E}^{\mathrm{in}}_r(\langle \tilde{\mathbb{T}} \rangle)$. By applying Lemma 4.5, there exists an element P_2 of A_r such that $\mathrm{MC}^{(r)}_{\lambda^{-1}}(\rho_{\mathbb{X}}) \cong F_{P_2} \circ MC^{(r)}_{\lambda^{-1}} \circ F_{P_1}(\rho_{\mathbb{Y}})$. According to Proposition 4.4, we have an isomorphism $F_{P_2} \circ MC^{(r)}_{\lambda^{-1}} \circ F_{P_1}(\rho_{\mathbb{Y}}) \cong \mathrm{MC}^{(r)}_{\lambda^{-1}} \circ F_{P_2P_1}(\rho_{\mathbb{Y}})$. By applying $\mathrm{MC}^{(r)}_{\lambda}$ to the above isomorphisms, we have an isomorphism $\rho_{\mathbb{X}} \cong F_{P_2P_1}(\rho_{\mathbb{Y}})$ (cf. Lemma 3.21). Thus there exists an element of $g \in GL(V)$ such that $[\mathbb{X}] = \mathrm{Inn}(g)(P_1P_2[\mathbb{Y}])$. Since $\langle \mathbb{X} \rangle = \langle \mathbb{Y} \rangle = \langle \tilde{\mathbb{T}} \rangle$, g is an element of $N_{GL(V)}(\langle \tilde{\mathbb{T}} \rangle)$. This completes the proof of the case of middle convolution functors.

The proof of the case of scalar multiplications is exactly same as the case of middle convolution functors. $\square$

By using the similar argument of Lemma 4.9, we obtain the following corollary.

Corollary 4.10. *Let r be a positive integer and $\mathbb{T} = (T_1, \dots, T_r)$ be an r-tuple of elements of $GL_n(\mathbb{F}_q)$ as Lemma 4.5. Let F be a functor which is an iterated composition of middle convolutions and scalar multiplications. Let $\tilde{\mathbb{T}} = (\tilde{T}_1, \dots, \tilde{T}_r)$ be an r-tuple of elements of $GL(V)$ which is defined by $\tilde{\mathbb{T}} := F(\mathbb{T})$.*

Here, V is the underlying $\mathbb{F}_q$-vector space of $\rho_{\tilde{\mathbb{T}}}$. Then $N_{GL(V)} \times A_r$ acts on $\mathcal{N}^{\mathrm{in}}_{\mathbb{T}}(\tilde{\mathbb{T}}, F)$ transitively. Here, V is the underlying $\mathbb{F}_q$-vector space of $\rho_{\tilde{\mathbb{T}}}$.

Theorem 4.11. *Let r be a positive integer and $\mathbb{T} := (T_1, \ldots, T_r)$ be an r-tuple of elements of $GL_n(\mathbb{F}_q)$ as Lemma 4.5. Let F be a functor which is an iterated composition of middle convolutions and scalar multiplications. Let $\tilde{\mathbb{T}} = (\tilde{T}_1, \ldots, \tilde{T}_r)$ be an r-tuple of elements of $GL(V)$ which is defined by $\tilde{\mathbb{T}} := F(\mathbb{T})$. Here, V is the underlying $\mathbb{F}_q$-vector space of $\rho_{\tilde{\mathbb{T}}}$. Let $\mathcal{C} = (C_1, \ldots, C_r)$ be the r-tuple of conjugacy classes of $\langle \tilde{\mathbb{T}} \rangle$ such that C_i contains $\tilde{T}_i$. Assume that $\mathcal{C}$ is rational and that there exists a subgroup H of $N_{GL_m(\mathbb{F}_q)}(\langle \tilde{\mathbb{T}} \rangle)$ such that the image of H in $N_{GL_m(\mathbb{F}_q)}(\langle \tilde{\mathbb{T}} \rangle)/\langle \tilde{\mathbb{T}} \rangle$ is equal to $N_{GL_m(\mathbb{F}_q)}(\langle \tilde{\mathbb{T}} \rangle)/\langle \tilde{\mathbb{T}} \rangle$ which satisfies one of the following conditions:*
(a) The group H is isomorphic to a product of $\mathbb{Z}/2\mathbb{Z}$.
(b) The group H is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2 \rtimes S_2 = D_4$ and the action of H on $\mathcal{E}^{\mathrm{in}}(\mathcal{C})$ factors through the canonical projection $H \twoheadrightarrow H/\langle (1,1) \rangle \cong (\mathbb{Z}/2\mathbb{Z})^2$.
Then the group $\langle \tilde{\mathbb{T}} \rangle / Z(\langle \tilde{\mathbb{T}} \rangle)$ is regular over $\mathbb{Q}$.

Proof. We consider the following diagram:

$$\begin{tikzcd}
\mathcal{U} \arrow[r, "j"] \arrow[dr, "f"'] & \mathbb{P}^1_{\mathbb{Q}} \times_{\mathbb{Q}} X \times_{\mathbb{Q}} \mathcal{U}_{\mathrm{r}} \arrow[d, "\bar{f}"] & \mathrm{pr}^*(D_r) \arrow[l, "i"'] \arrow[dl, "\tilde{f}"] & \mathrm{pr}^*((*)_{\mathcal{U}_r, D_r}) \\
 & X \times_{\mathbb{Q}} \mathcal{U}_r . & &
\end{tikzcd}$$

Here X is a product of $\mathbb{G}_{m,\mathbb{Q}}$ in the case of (a), $({\mathbb{G}_{m,\mathbb{Q}}}^2/S_2)$ in the case of (b) and $\mathrm{pr}^*((*)_{\mathcal{U}_r,D_r})$ is the pull back of the universal simple divisor by the second projection $\mathrm{pr} : X \times_{\mathbb{Q}} \mathcal{U}_r \to \mathcal{U}_r$. Then there exists a group homomorphism $\phi : \pi_1^{\mathrm{et}}(\mathcal{U}_r \times_{\mathbb{Q}} X, \bar{x}) \twoheadrightarrow \pi_1^{\mathrm{et}}(X, \bar{x}) \twoheadrightarrow H \subset N_{GL_m(\mathbb{F}_q)}(\langle \tilde{\mathbb{T}} \rangle) \to \mathrm{Aut}(\langle \tilde{\mathbb{T}} \rangle)$ such that $\phi(G_{\mathbb{Q}}) = 1$. Here, $\bar{x}$ is a geometric point of $\mathcal{U}_r \times_{\mathbb{Q}} X$ lying over a $\mathbb{Q}$-rational point x of $\mathcal{U}_r \times_{\mathbb{Q}} X$. Let $\mathcal{H}^{\mathrm{in}}(X \times_{\mathbb{Q}} \mathcal{U}_r, \mathrm{pr}^*(D_r), \phi)$ be the Hurwitz space which is defined by the diagram $\mathrm{pr}^*((*)_{\mathcal{U}_r,D_r})$ and the group homomorphism ϕ. We identify the fiber of the morphism $\mathcal{H}^{\mathrm{in}}(X \times_{\mathbb{Q}} \mathcal{U}_r, \mathrm{pr}^*(D_r), \phi)$ at $\bar{x}$ with the $\pi_1^{\mathrm{et}}(X \times_{\mathbb{Q}} \mathcal{U}_r, \bar{x})$-set $\mathcal{E}_r^{\mathrm{in}}(\langle \tilde{\mathbb{T}} \rangle)$ (cf. Lemma 2.2). Note that $G_{\mathbb{Q}}$ acts on $\mathcal{N}^{\mathrm{in}}_{\mathbb{T}}(\tilde{\mathbb{T}}, F)$ because $\mathcal{C}$ is rational and the action of $G_{\mathbb{Q}}$ does not exchange the image of the geometric fundamental group of the punctured projective line. Let $\mathcal{H}^{\mathrm{in}}(\mathcal{N}^{\mathrm{in}}_{\mathbb{T}}(\tilde{\mathbb{T}}, F))$ be the subscheme of $\mathcal{H}^{\mathrm{in}}(X \times_{\mathbb{Q}} \mathcal{U}_r, \mathrm{pr}^*(D_r), \phi)$ which corresponds to the sub-$\pi_1(X \times_{\mathbb{Q}} \mathcal{U}_r)$-set $\mathcal{N}^{\mathrm{in}}_{\mathbb{T}}(\tilde{\mathbb{T}}, F)$ of $\mathcal{E}_r^{\mathrm{in}}(\langle \tilde{\mathbb{T}} \rangle)$ (cf. Definition 2.16). According to Corollary 4.10, $\mathcal{H}^{\mathrm{in}}(\mathcal{N}^{\mathrm{in}}_{\mathbb{T}}(\tilde{\mathbb{T}}, F))$ is geometrically connected. Since the scheme $\mathcal{H}^{\mathrm{in}}(\mathcal{N}^{\mathrm{in}}_{\mathbb{T}}(\tilde{\mathbb{T}}, F))$ is finite etale over $X \times_{\mathbb{Q}} \mathcal{U}_r$, there exists an isomorphism $\mathcal{H}^{\mathrm{in}}(\mathcal{N}^{\mathrm{in}}_{\mathbb{T}}(\tilde{\mathbb{T}}, F)) \cong Y \times_{\mathbb{Q}} W$ over $X \times_{\mathbb{Q}} \mathcal{U}_r$ where Y (resp. W) is geometrically connected and finite etale over X (resp. $\mathcal{U}_r$). It proved in the paper [D-R, p 783.] that the genus of the j-th braid orbit of $[\tilde{\mathbb{T}}] \in \mathcal{E}_r^{\mathrm{in}}(\langle \tilde{\mathbb{T}} \rangle)$ in the sense of [M-M, Section 3, 5.2.] is equal

to 0 for each $j = 3, \dots k+2$ and the oddness condition for $[\tilde{\mathbb{T}}]$ in the sense of [M-M, Section 3, 5.3.] is satisfied. Hence, W is a rational variety over $\mathbb{Q}$. Since Y is a product of double covering of $\mathbb{G}_{m,\mathbb{Q}}$, $\mathcal{H}^{\mathrm{in}}(\mathcal{N}_{\mathbb{T}}^{\mathrm{in}}(\tilde{\mathbb{T}}, F))$ is a rational variety over $\mathbb{Q}$ according to [M-M, Section 3, Theorem 5.7.]. In particular, we have $\mathcal{H}^{\mathrm{in}}(X \times_{\mathbb{Q}} \mathcal{U}_r, \mathrm{pr}^*(D_r), \phi)(\mathbb{Q}) \neq \emptyset$. By applying Corollary 2.20, we complete the proof of the theorem. □

4.2 Realization of Some Orthogonal Groups (2)

We realize some finite orthogonal groups as Galois groups over $\mathbb{Q}$. We use tuples of elements of $GL_2(\mathbb{F}_q)$ which are not linearly rigid.

Proposition 4.12. *Let p be an odd prime and n be an even natural number. If $p \equiv 7 \pmod{12}$,$4 \nmid n$ and $n \geq 12$ hold, then $PSO_n^+(\mathbb{F}_p)$ is regular over $\mathbb{Q}$.*

Proof. Take a $(2m+4)$-tuple of elements $\mathbb{T}_1$ of $GL_2(\mathbb{F}_p)$ as follows:

$$\mathbb{T}_1 := (-E_2, \dots, -E_2, g_1, g_1^{-1}, g_2, -g_2^{-1}).$$

Here g_1 and g_2 are defined by equations (6) and (7) and E_2 is the identity matrix of degree 2. Note that $\mathbb{T}_1$ is not linearly rigid because the index of rigidity of $(\mathbb{T}_1, -E_2)$ is equal to 0.

Let $(U_1, \dots, U_{2m}, G_1, G_2, G_3, G_4)$ be a $(2m+4)$-tuple of elements of $GL(W_1)$ which is defined as follows:

$$(U_1, \dots, U_{2m}, G_1, G_2, G_3, G_4) := \mathrm{MC}_{-1}^{(2m+4)}(\mathbb{T}_1)$$

where W_1 is the underlying $\mathbb{F}_p$-vector space of $\mathrm{MC}_{-1}^{(2m+4)}(\rho_{\mathbb{T}_1})$. We denote the $(2m+4)$-tuple $(-U_1, U_2, \dots, U_{2m}, G_1, G_2, G_3, G_4)$ by $\tilde{\mathbb{T}}_1$ for short. According to Lemma 3.21, we have $-U_1 \cdots U_{2m} G_1 G_2 G_3 G_4 = \mathrm{Id}_{W_1}$. The dimension of W_1 over $\mathbb{F}_p$ is equal to $2(2m+3)$ (cf. Lemma 3.18).

By the same argument as the proof of Claim 1 in the proof of Proposition 3.35, there exists a symmetric form $(\ ,\ )_1$ on W_1 such that $\langle \tilde{\mathbb{T}}_1 \rangle = SO(W_1, (\ ,\ )_1) \cong SO^+_{2(2m+3)}(\mathbb{F}_p)$.

Let $C(U_i)$, $i = 1, \dots, 2m$ (resp. $C(G_j)$, $j = 1, 2, 3, 4$) be the conjugacy class of $\langle \tilde{\mathbb{T}}_1 \rangle$ which contains U_i(resp. G_j). Since $C(U_i)$ and $C(G_j)$ are rational for $i = 1, \dots, 2m$, $j = 1, 2$ and $C(G_3)^3 = C(G_4)$, the $(2m+4)$-tuple of conjugacy classes $(-C(U_1), \dots, C(U_{2m}), C(G_1), C(G_2), C(G_3), C(G_4))$ is rational (see Claim 2 in the proof of Proposition 3.35).

Let $\{v_1, \dots, v_{2m+3}, v'_1, \dots, v'_{2m+3}\}$ be a standard basis of $(W_1, (\ ,\ )_1)$ in the sense of [K-L, Proposition 1.2, 5.3.(1)]. According to [K-L, Proposition 1.2, 7.3 (3)], the outer automorphism group of $SO(W_1, (\ ,\ )_1)$ is generated by the images of δ_1 , γ_1 where $\gamma_1 \in GO(W_1, (\ ,\ )_1)$ is a reflection and

$$\delta_1 : v_i \mapsto -v_i\ ,\ v'_i \mapsto v'_i\ ,\ i = 1, \dots, 2m+3.$$

Let H_1 be the group which is generated by γ_1, δ_1. The group H_1 is isomorphic to D_4. The action of H_1 on $\mathcal{E}^{\mathrm{in}}_{2m+4}(\langle \tilde{\mathbb{T}}_1 \rangle)$ factors through the canonical projection $H \twoheadrightarrow H / \langle (\gamma_1 \delta_1)^2 \rangle \cong (\mathbb{Z}/2\mathbb{Z})^2$. By applying Theorem 4.11 with $r = 2m+4$, $H = H_1$ and $\tilde{\mathbb{T}} = \tilde{\mathbb{T}}_1$, we deduce the conclusion of the proposition. □

From Proposition 3.35 and Proposition 4.12, we have the following corollary.

Corollary 4.13. *Let p be an odd prime and n be an even natural number. If $p \equiv 7 \pmod{12}$ and $n \geq 12$ hold, then $PSO_n^+(\mathbb{F}_p)$ is regular over $\mathbb{Q}$.*

Proposition 4.14. *Let q be a power of odd prime and n be an even natural number. If $n > max\{\varphi(q-1), 7\}$, $\frac{n}{2} \equiv \frac{\varphi(q-1)}{2} + 1 \pmod 2$ and $q \equiv 3 \pmod 4$, then $PSO_n^+(\mathbb{F}_q)$ is regular over $\mathbb{Q}$.*

Proof. Let $\alpha \in \mathbb{F}_q$ be a generator of $\mathbb{F}_q^\times$ and put $k := \frac{\varphi(q-1)}{2}$. Put

$$S_i := \begin{pmatrix} -\alpha_i & 0 \\ 0 & -\alpha_i^{-1} \end{pmatrix} \ 1 \leq i \leq k \tag{13}$$

and

$$R := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \tag{14}$$

where $\{\alpha_i, \alpha_i^{-1}\}_{1 \leq i \leq k}$ runs generators of $\mathbb{F}_q^\times$. Take a $(2m + k + 2)$-tuple $\mathbb{T}_2$ of elements of $GL_2(\mathbb{F}_q)$ as follows:

$$\mathbb{T}_2 := (-1, -1 \cdots -1, S_1, \ldots, S_k, R, -S_\infty^{-1} R^{-1})$$

where $S_\infty^{-1} := \prod_{i=1}^{k} S_i$.

Let $(U_1, \ldots, U_{2m}, \tilde{S}_1, \ldots, \tilde{S}_r, \tilde{T}_1, \tilde{T}_2)$ be a (2m+k+2)-tuple of elements of $GL(W_2)$ which is defined as follows:

$$(U_1, \ldots, U_{2m}, \tilde{S}_1, \ldots, \tilde{S}_r, \tilde{T}_1, \tilde{T}_2) := MC_{-1}^{(2m+k+2)}(\mathbb{T}_2)$$

where W_2 is the underlying $\mathbb{F}_q$-vector space of $\mathrm{MC}_{-1}^{(2m+4)}(\rho_{\mathbb{T}_2})$. By using the explicit description of middle convolution functors and Lemma 3.21, we conclude that U_i are unipotent biperspectivities and $\tilde{S}_i$ are semi-simple biperspectivities of eigenvalues α_i, α_i^{-1} and $\tilde{T}_i$ are elements of order 4. The dimension of W_2 over $\mathbb{F}_q$ is equal to $(4m + 2k + 2)$ (cf. Lemma 3.18). We denote the $(2m + k + 2)$-tuple $(-U_1, U_2, \ldots, U_{2m}, \tilde{S}_1, \ldots, \tilde{S}_r, \tilde{T}_1, \tilde{T}_2)$ by $\tilde{\mathbb{T}}_2$ for short. After the exactly same arguments as the proof of Claim 1 and Claim 2 in the proof of Proposition 3.35, there exists a symmetric form $(\ ,\ )_2$ on W_2 such that $\langle \tilde{\mathbb{T}}_2 \rangle = SO(W_2, (\ ,\ )_2) \cong SO^+_{4m+2k;+2}(\mathbb{F}_q)$ and the $(2m + k + 2)$-tuple $(-C(U_1), C(U_2) \ldots, C(U_{2m}), C(\tilde{S}_1), \ldots, C(\tilde{S}_r), C(\tilde{T}_1), C(\tilde{T}_2))$ of the conjugacy classes of $\langle \tilde{\mathbb{T}}_2 \rangle$ is rational. Here $C(U_i)$ (resp. $C(\tilde{S}_j)$, resp. $C(\tilde{T}_k)$) is the conjugacy class of $\langle \tilde{\mathbb{T}}_2 \rangle$ which contains U_i (resp. $\tilde{S}_j$, resp. $\tilde{T}_k$).

Let $\{u_1, \ldots, u_{2m+k+1}, u'_1, \ldots, u'_{2m+k+1}\}$ be a standard basis of $(W_2, (\ ,\ )_2)$ in the sense of [K-L, Proposition 1.2, 5.3.(1)]. According to [K-L, Proposition 1.2, 7.3 (3)], the outer automorphism group of $SO(W_2, (\ ,\ )_2)$ is generated by the images of δ_2 , γ_2 where $\gamma_2 \in GO(W_2, (\ ,\ )_2)$ is a reflection and

$$\delta_2 : u_i \mapsto -u_i\ ,\ u'_i \mapsto u'_i\ ,\ i = 1, \ldots, 2m + k + 1.$$

Let H_2 be the group which is generated by γ_2, δ_2. The group H_2 is isomorphic to D_4. The action of H_2 on $\mathcal{E}^{\mathrm{in}}_{2m+k+2}(\langle\, \tilde{\mathbb{T}}_1 \,\rangle)$ factors through the canonical projection $H \twoheadrightarrow H/\,\langle(\gamma_2\delta_2)^2\,\rangle \cong (\mathbb{Z}\,/2\,\mathbb{Z})^2$

By applying Theorem 4.11 with $r = 2m + k + 2$, $H = H_2$ and $\tilde{\mathbb{T}} = \tilde{\mathbb{T}}_2$, we deduce the conclusion of the proposition. $\square$

References

[D-R] Dettweiler,M. Reiter,S. An Algorithm of Katz and its Application to the Inverse Galois Problem *J.Symbolic Computation*(2000)**30**, 761-798.

[Fu] Fulton,W. Hurwitz schemes and irreducibility of moduli spaces of algebraic curves. *Ann.math***90**,(1969)542-575.

[Fr-Vö] Fried,M.,and H. Völklein. The inverse Galios problem and rational points on moduli spaces.*Math. Ann.***290**,(1991) 771-800.

[K-L] Kleidman, P. Liebeck M. The subgroup Structure of the Finite Classical Groups. Cambridge,U.K., Cambridge University Press.

[M-M] Malle,Matzat. The inverse Galois problem ,Prinston University Press,(1980).

[Liu] Liu, Qing. Algebraic gepmetry and arithmetic surfaces, Oxford Science Publications,(2001).

[SGA1] A.Grothendieck,Séminaire de Géométrie Algébrique du Bois Marie 1960/1961 SGA1,Springer Lecture Notes on Math 224,(1971).

[Se] J-P. Serre, Topics in Galois Theory. *A K Peters,Ltd. Wellesley,MA* (2008).

[Th] Thompson,J.G.Some finite groups which appears Gal(L/K) where K $\subset$ $\mathbb{Q}(\mu_n)$. *J.Algebra***89**(1984),437-499

[Vö] H.Völklein. Groups as Galios Groups *Cambridge Studies in AdvancedMathematics* **53**(1996)

[W] Wagner,A. Collieation groups generated by homologies of order greater than 2.*Geom. Ded.*,*7*,387-389(1978).